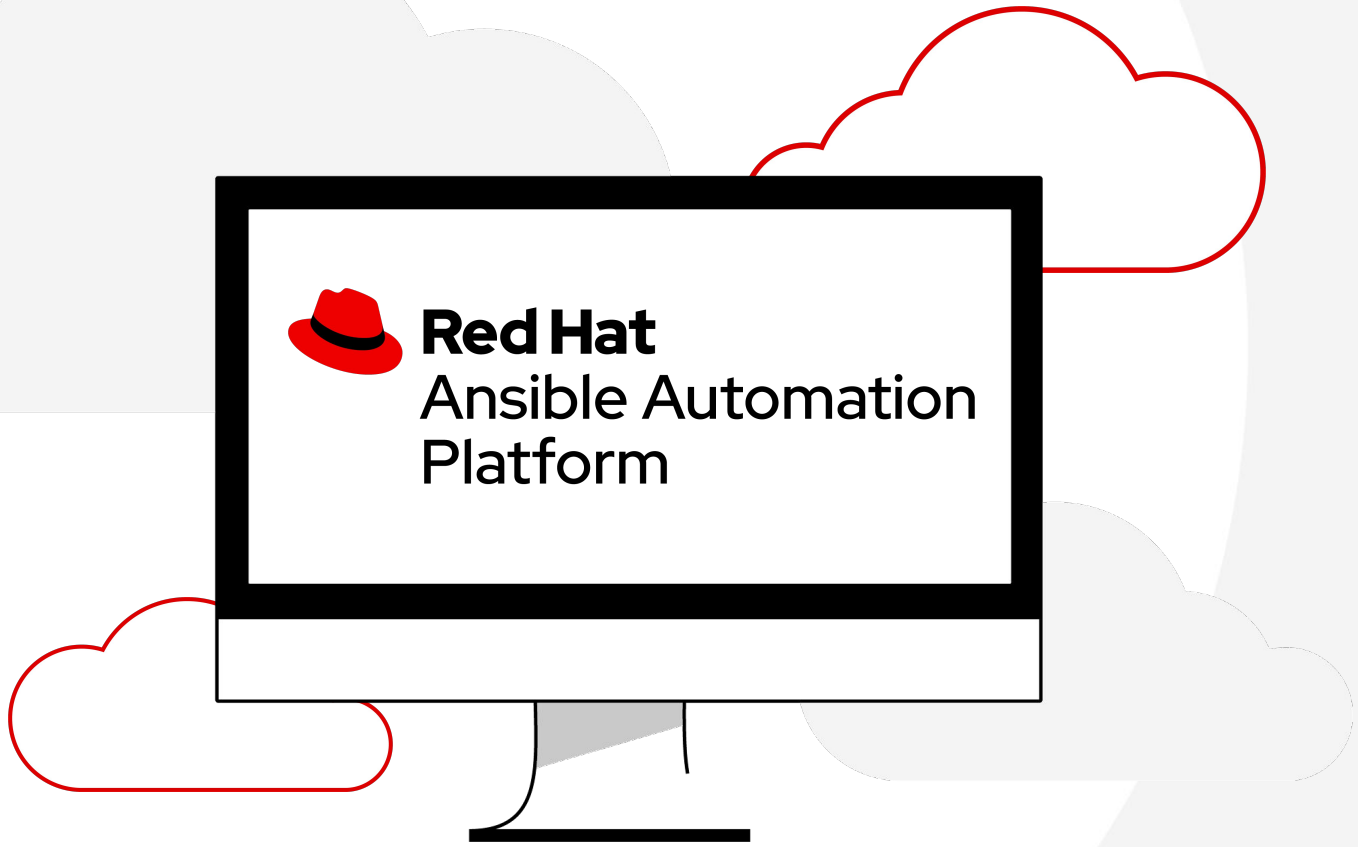
Red Hat
Ansible Automation
Platform

Ansible Security automation workshop

Introduction to Ansible security automation for security teams

Housekeeping

- Timing
- Breaks
- Takeaways



What you will learn

Introduction

- Introducing Ansible Automation Platform
- Ansible security automation overview

Section 1

- Exploring the lab environment
- Ansible Automation Platform basics
- Lab exercises

Section 2

- Security personas
- Automation controller basics
- Lab exercises

Section 3

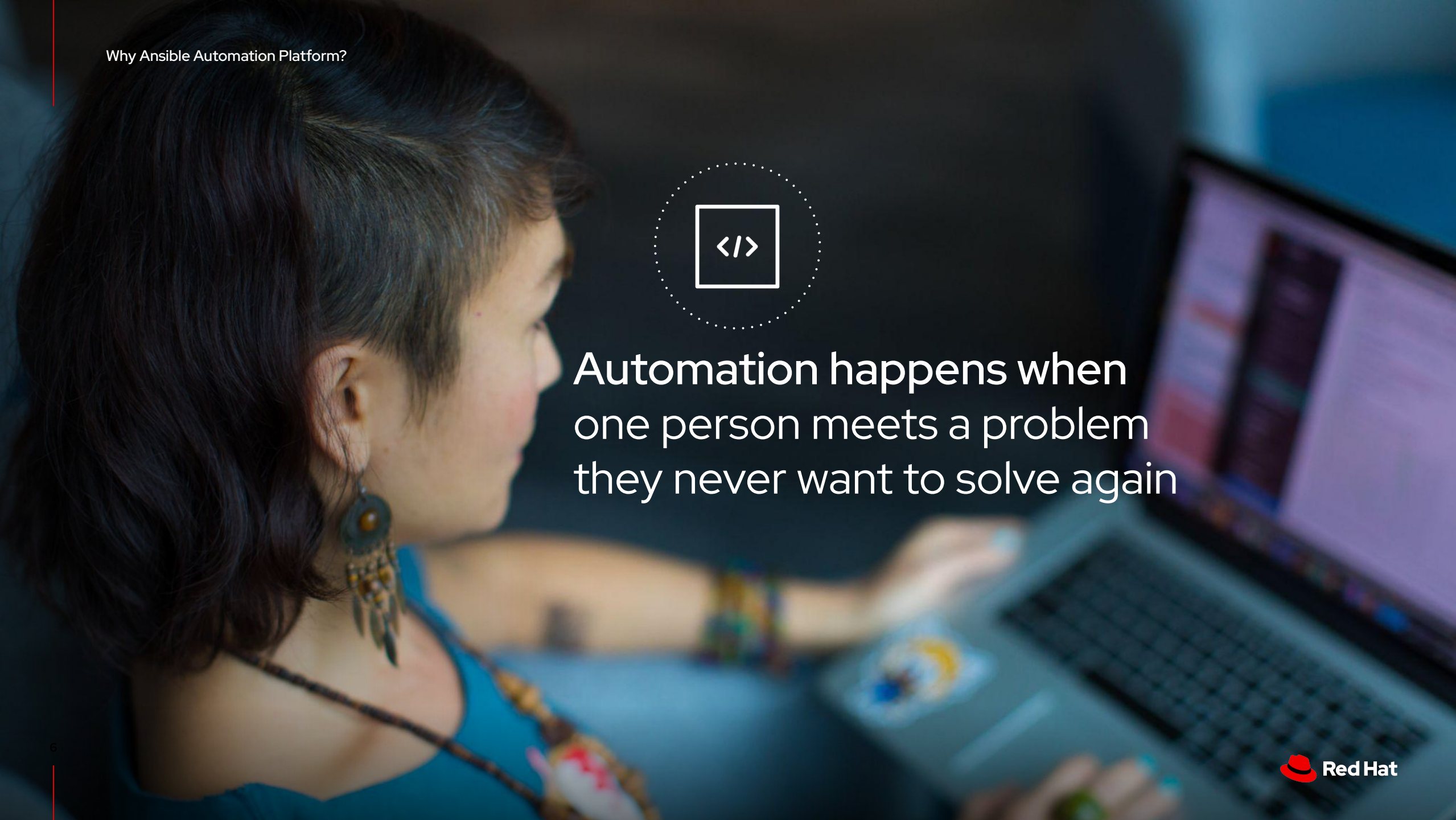
- Wrapping up

Introduction

Topics Covered:

- Why Ansible Automation Platform?
- Ansible security automation overview

Why Ansible Automation Platform?

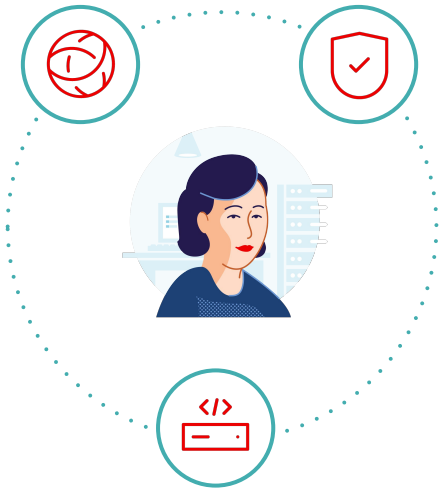


Automation happens when one person meets a problem they never want to solve again

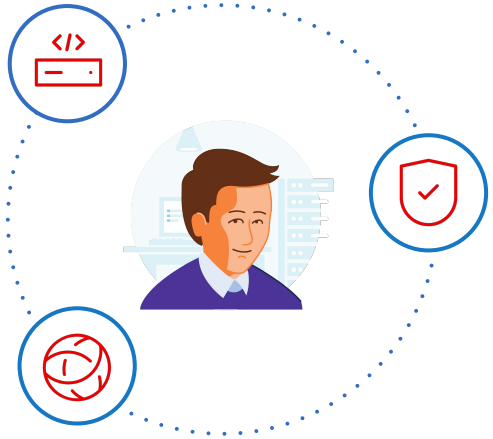
Red Hat

Many organizations share the same challenge

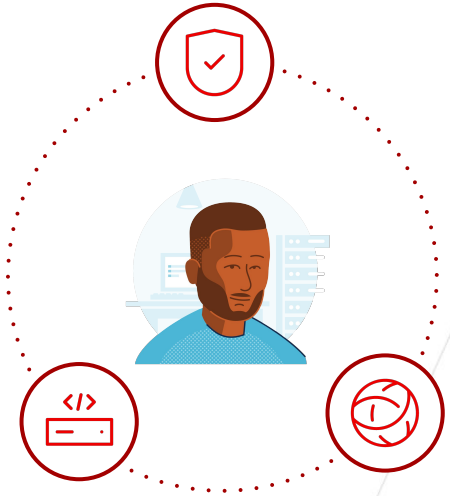
Too many unintegrated, domain-specific tools



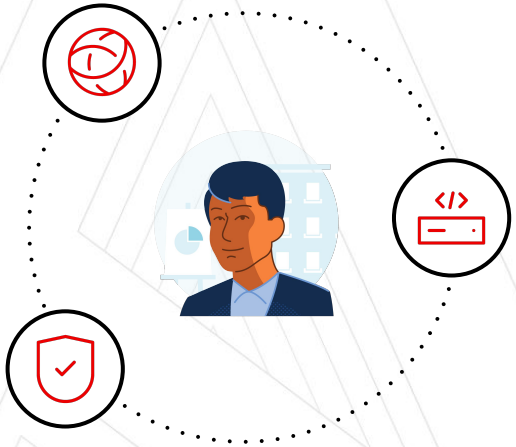
Network ops



SecOps

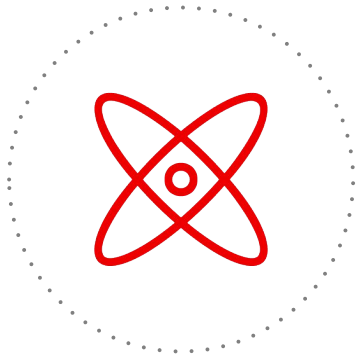


Devs/DevOps



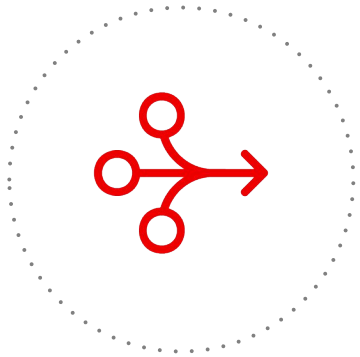
IT ops

Why the Ansible Automation Platform?



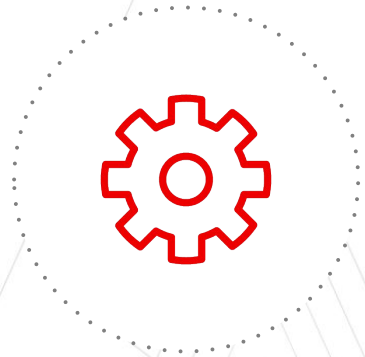
Powerful

Orchestrate complex processes at enterprise scale.



Simple

Simplify automation creation and management across multiple domains.

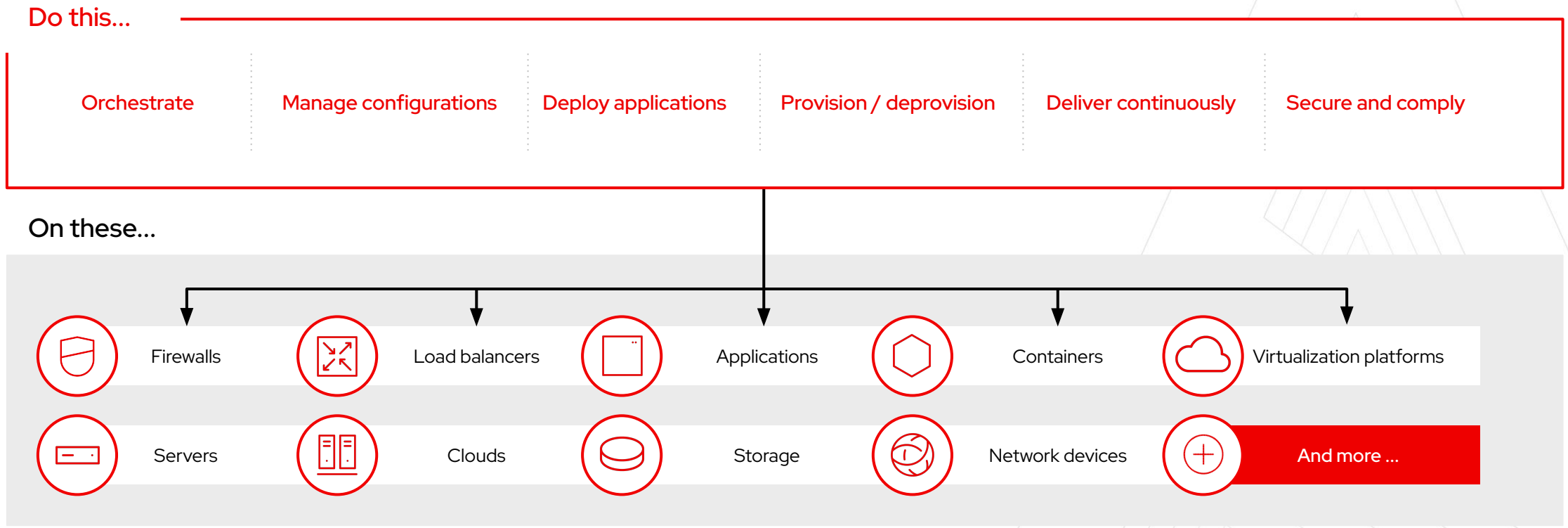


Agentless

Easily integrate with hybrid environments.

Automate the deployment and management of automation

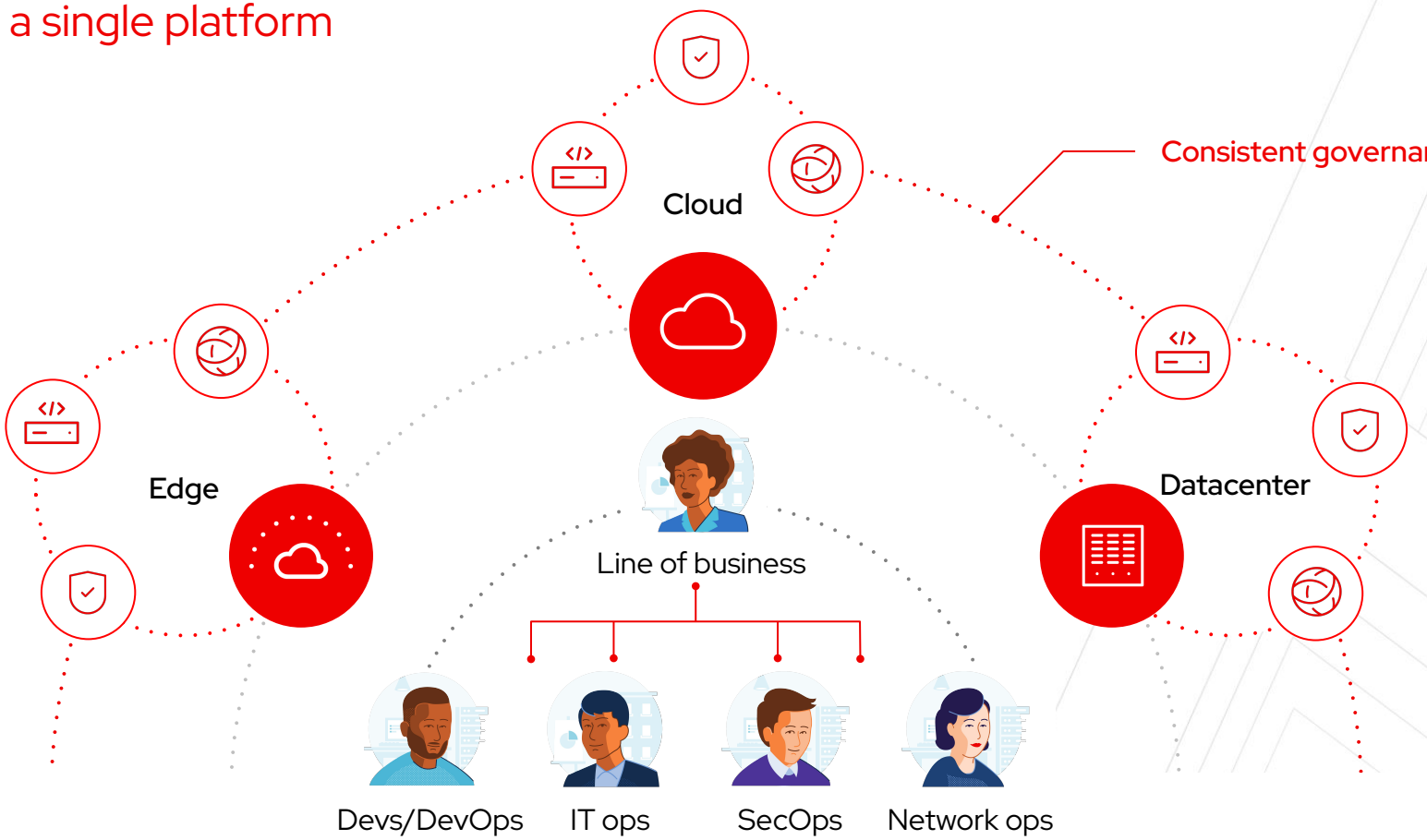
Your entire IT footprint



Red Hat
Ansible Automation
Platform

Break down silos

Different teams a single platform



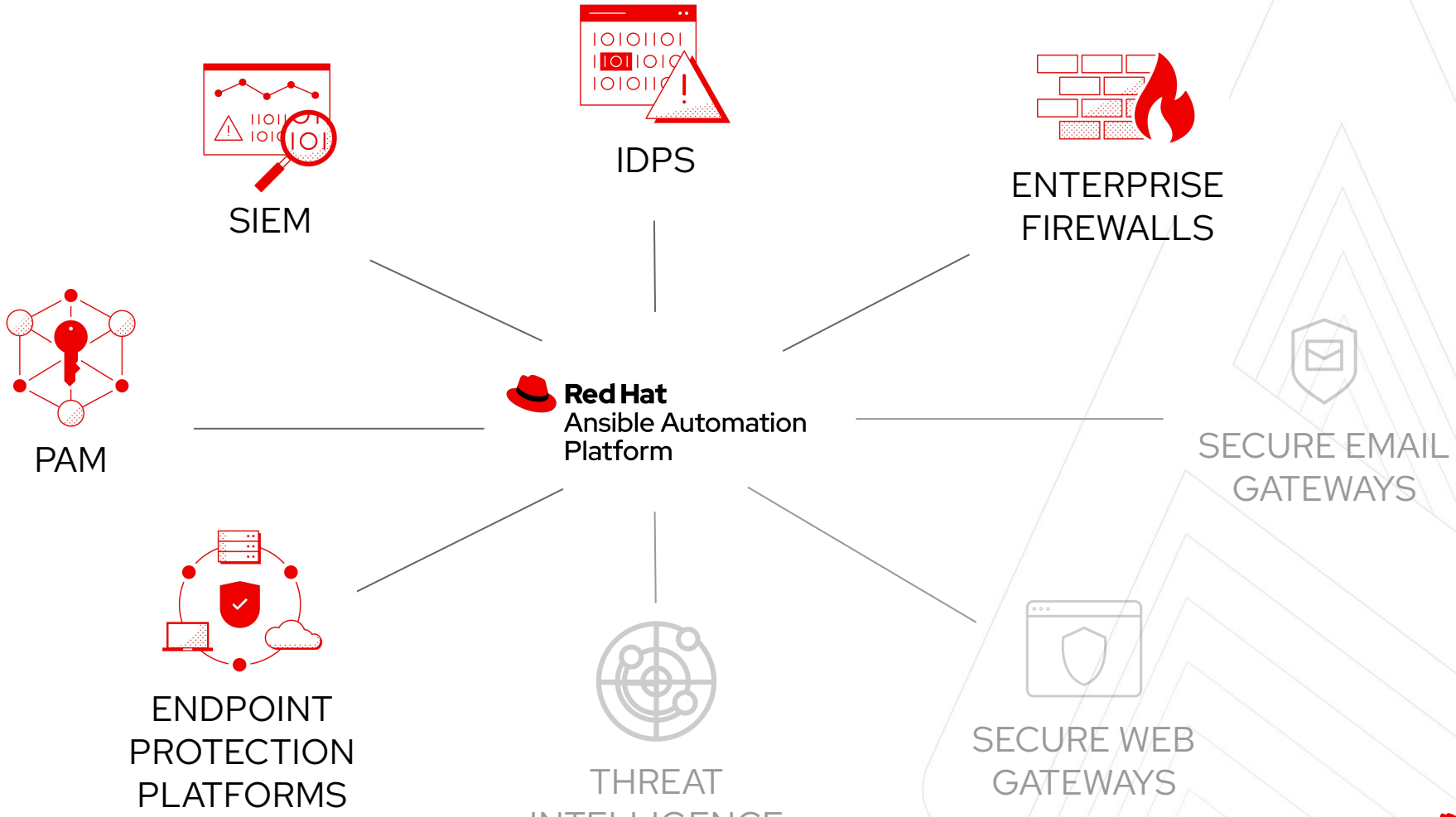
What is Ansible security automation?

What Is Ansible security automation?

Ansible security automation is our expansion deeper into the security use case. The goal is to provide a more efficient, streamlined way for security teams to automate their various processes for the identification, search, and response to security events. This is more complex and higher-value than the application of a security baseline (PCI, STIG, CIS) to a server.

Ansible security automation is a supported set of Ansible modules, roles and playbooks designed to unify the security response to cyberattacks.

What Ansible security automation covers



Red Hat
Ansible Automation
Platform

Is It A Security Solution?

No. Ansible can help Security teams “stitch together” the numerous security solutions and tools already in their IT environment for a more effective cyber defense.

By automating security capabilities, organizations can better unify responses to cyberattacks through the coordination of multiple, disparate security solutions, helping these technologies to act as one in the face of an IT security event.

Red Hat will not become a security vendor, we want to be a security enabler.

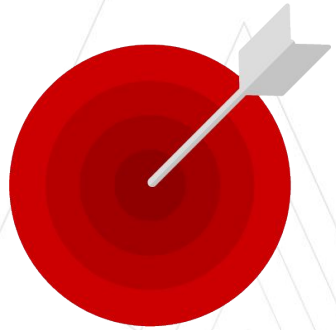
What Does It Do?

Investigation Enrichment

Enabling programmatic access to log configurations such as destination, verbosity, etc.

Threat Hunting

Automate alerts, correlation searches and signature manipulation to preemptively identify threats



Incident Response

Creating new security policies to grant access, block or quarantine a machine

Ansible Security Ecosystem

Security Information & Events Management

splunk>

IBM

Enterprise Firewalls

Check Point SOFTWARE TECHNOLOGIES LTD

CISCO

f5

FORTINET

JUNIPER NETWORKS

Intrusion Detection & Prevention Systems

SNORT

Check Point SOFTWARE TECHNOLOGIES LTD

FORTINET

Privileged Access Management

CYBERARK

syncope

IBM

Endpoint Protection

Symantec

TREND MICRO

Red Hat

Section 1

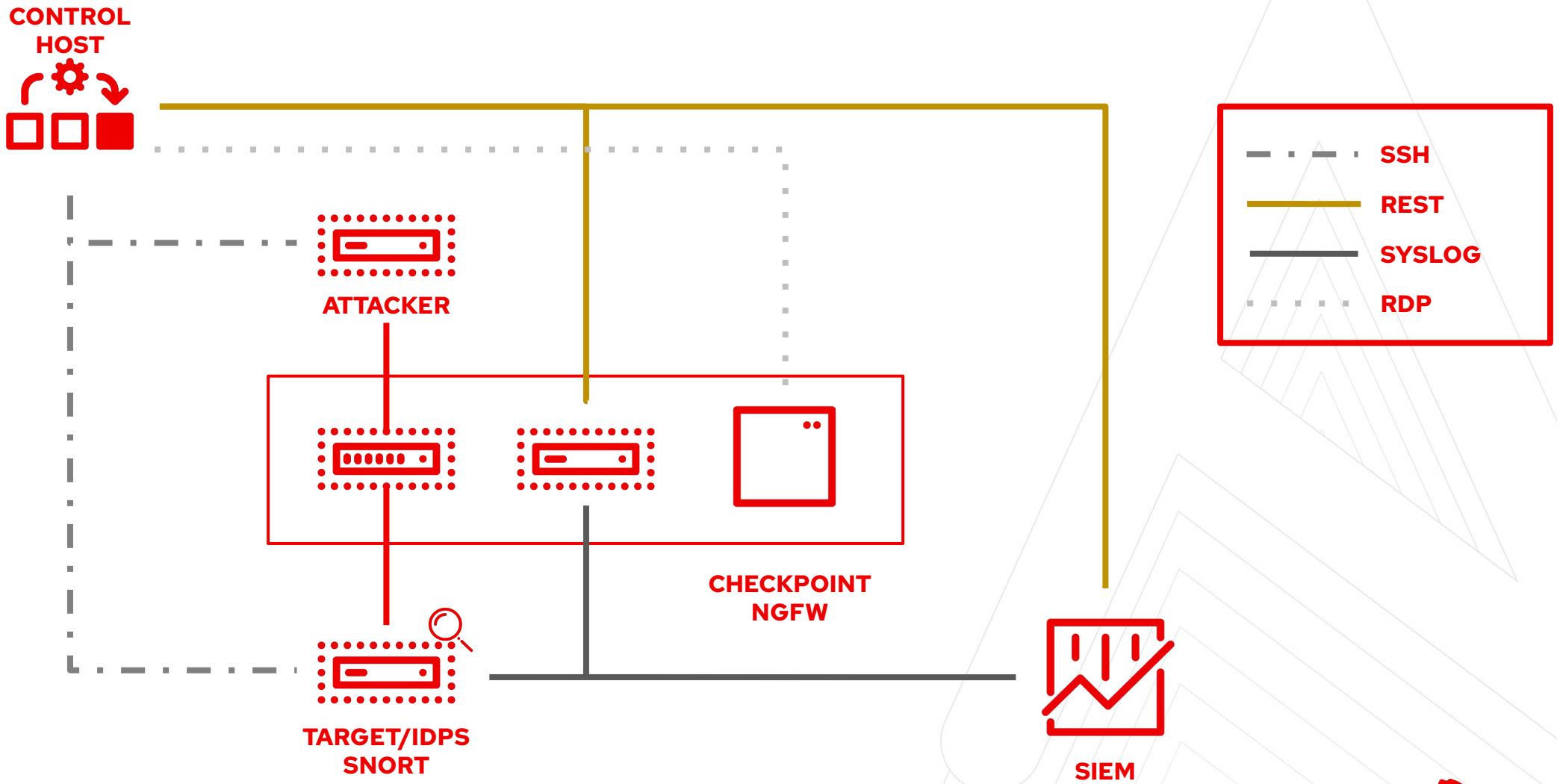
Introduction to Ansible security automation basics

Exercise 1.1

Topics Covered:

- Exploring the lab environment
- What are Automation execution environments?
- Automation content navigator (*ansible-navigator*)
- Workshop inventory overview

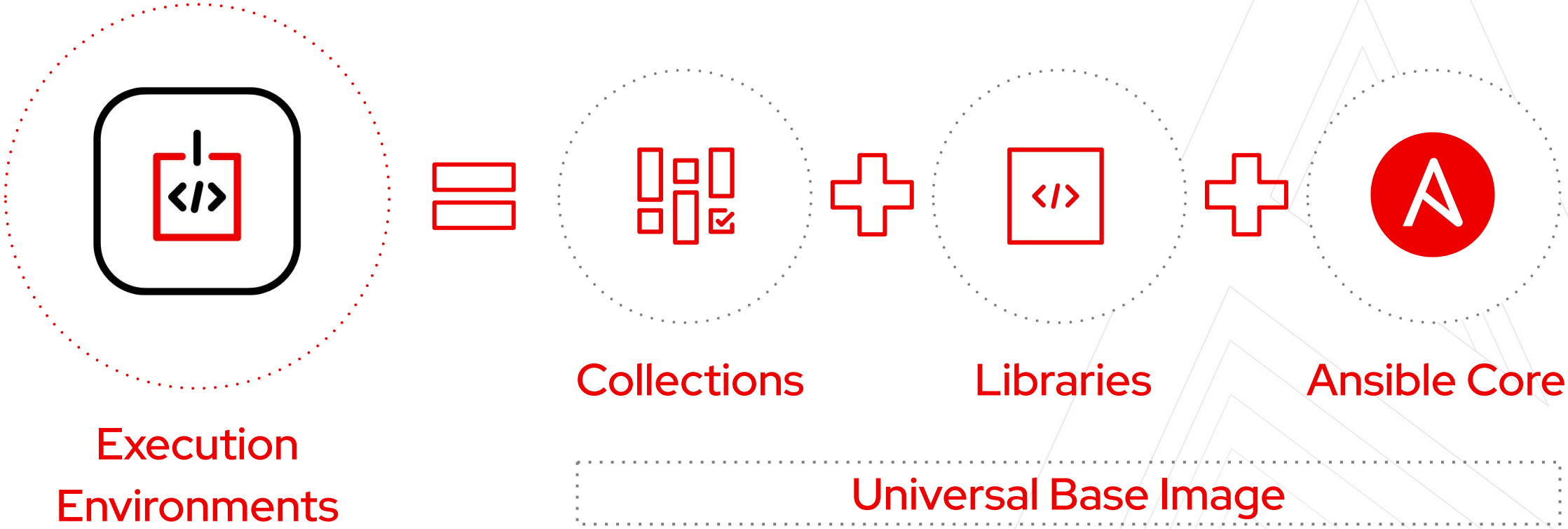
Security workshop architecture



What are Automation execution environments?

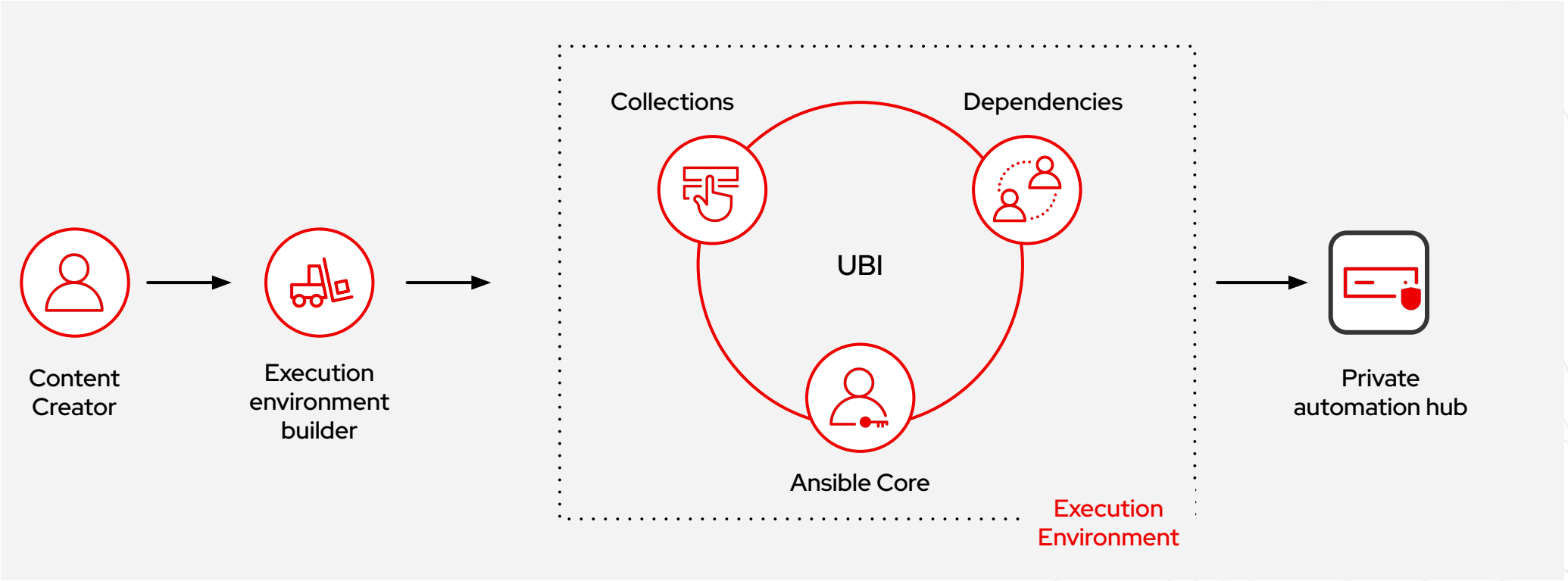
Automation execution environments

Components needed for automation, packaged in a cloud-native way



Build, create, publish

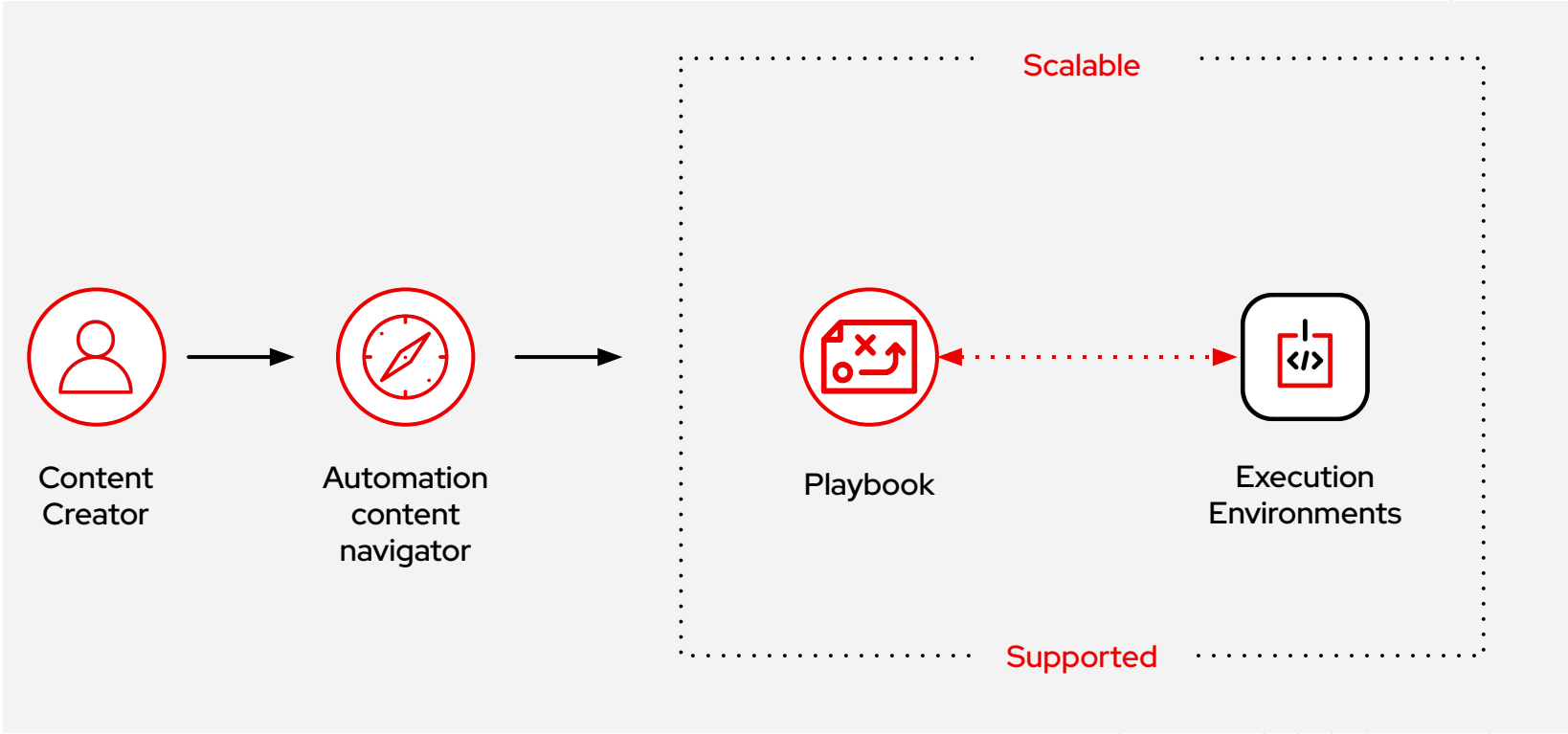
Development cycle of an automation execution environment



Red Hat

Develop, test, run

How to develop, test and run containerized Ansible content



Workshop Automation execution environment

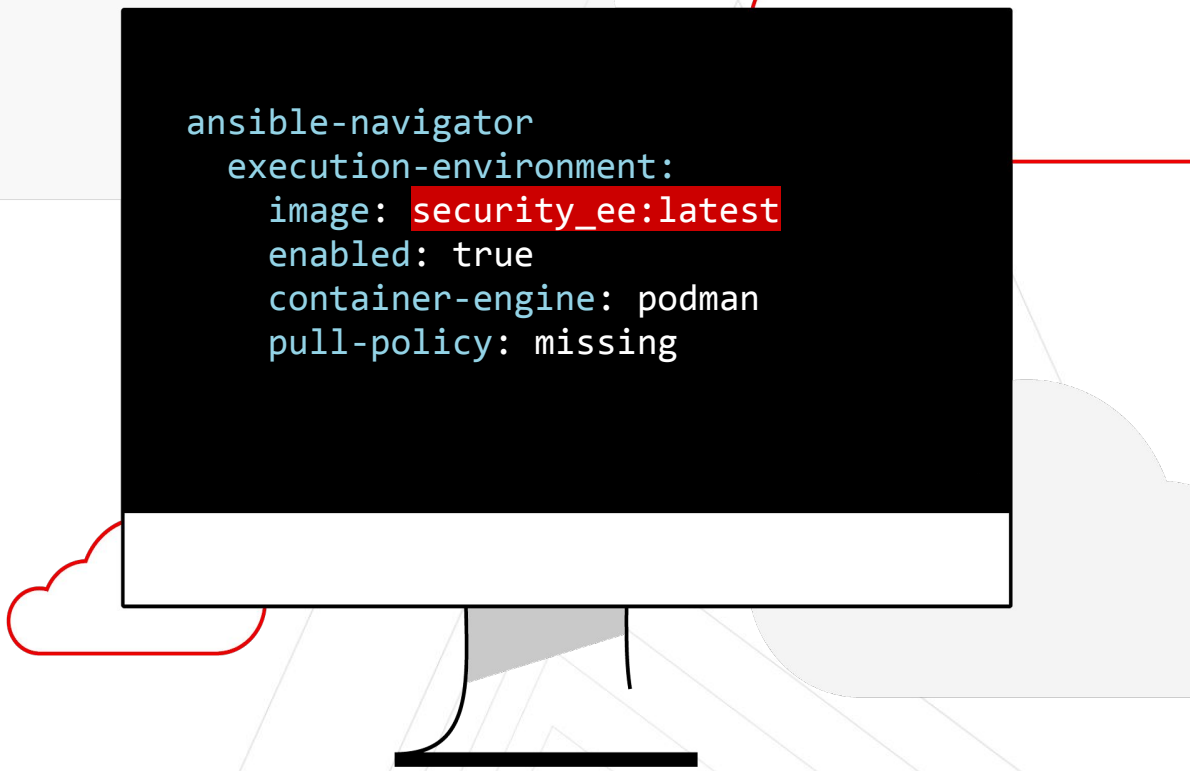
Ansible Security Roles and Automation content collections already available

Do I need to do anything? No

- Everything has been set up for you and ready to use.
- All Content Collections and Roles are included.
- `ansible-navigator` configuration preconfigured

What's included?

- We will use `ansible-navigator` to explore the `security_ee` content



Automation content navigator *(ansible-navigator)*

ansible-navigator

Using the latest ansible-navigator command

What is ansible-navigator?

ansible-navigator command line utility and text-based user interface (TUI) for running and developing Ansible automation content.

It replaces the previous command used to run playbooks “ansible-playbook”.

ansible-navigator

Mapping to previous Ansible commands

ansible command	ansible-navigator command
`ansible-config`	`ansible-navigator config`
`ansible-doc`	`ansible-navigator doc`
`ansible-inventory`	`ansible-navigator inventory`
`ansible-playbook`	`ansible-navigator run`

How do I use ansible-navigator?

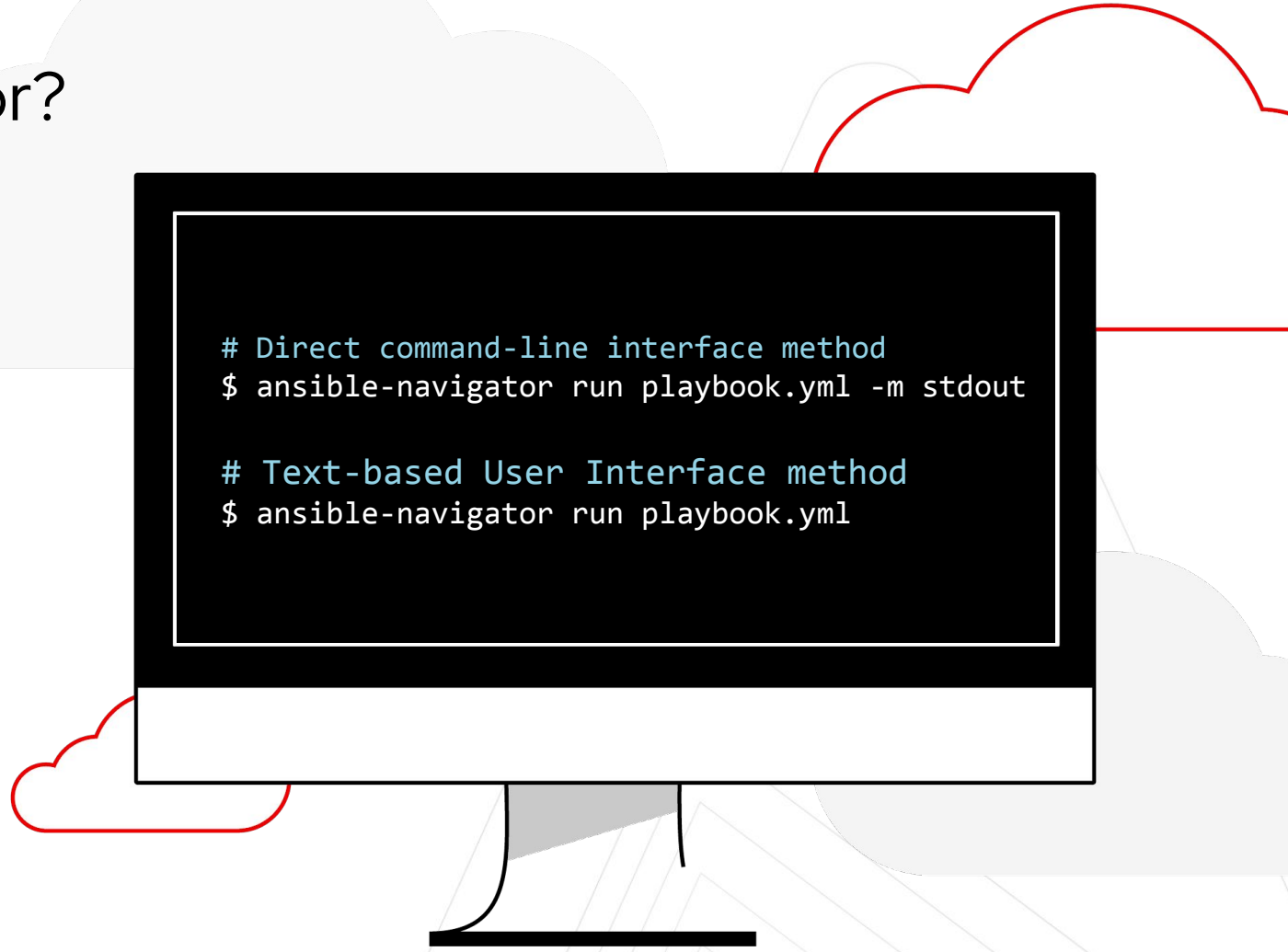
Hello ansible-navigator

How do I use ansible-navigator?

As previously mentioned, it replaces the ansible-playbook command.

As such it brings two methods of running playbooks:

- Direct command-line interface
- Text-based User Interface (TUI)



Workshop inventory

Security workshop inventory

The Basics

- Contains all machines of your environment
- Setup up just for you, individually
- Note your individual IP addresses for each machine
- The exercises needs you to replace example IP addresses with your individual ones
- `/home/student<X>/lab_inventory/hosts`

Workshop inventory - Groups

Ansible Inventory - Groups

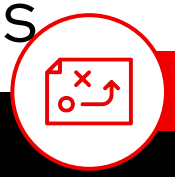
```
[all:vars]
ansible_user=student1
ansible_ssh_pass=ansible
ansible_port=22

[control]
ansible ansible_host=22.33.44.55 ansible_user=ec2-user private_ip=192.168.2.3

[siem]
qradar ansible_host=22.44.55.77 ansible_user=admin private_ip=172.16.3.44
ansible_httpapi_pass="Ansible1!" ansible_connection=httpapi ansible_httpapi_use_ssl=yes
ansible_httpapi_validate_certs=False ansible_network_os=ibm.qradar.qradar

[ids]
snort ansible_host=33.44.55.66 ansible_user=ec2-user private_ip=192.168.3.4
```

Workshop inventory - Variables



Ansible Inventory - Variables

```
[all:vars]
ansible_user=student1
ansible_ssh_pass=ansible
ansible_port=22

[control]
ansible ansible_host=22.33.44.55 ansible_user=ec2-user private_ip=192.168.2.3

[siem]
qradar ansible_host=22.44.55.77 ansible_user=admin private_ip=172.16.3.44
ansible_httpapi_pass="Ansible1!" ansible_connection=httpapi ansible_httpapi_use_ssl=yes
ansible_httpapi_validate_certs=False ansible_network_os=ibm.qradar.qradar

[ids]
snort ansible_host=33.44.55.66 ansible_user=ec2-user private_ip=192.168.3.4
```

Exercise Time!

Do Exercise 1.1 in your lab environment

- Follow the steps to access your environment
- Your environment will have unique IP addresses and DNS names.

  The screenshots are only examples
- Access to machines is done via the VS Code Online editor using the

  built-in terminal

Exercise 1.2

Topics Covered:

- Managing Check Point Next Generation Firewalls
- Ansible Playbook basics
- Running your first playbook

Managing Check Point Firewalls

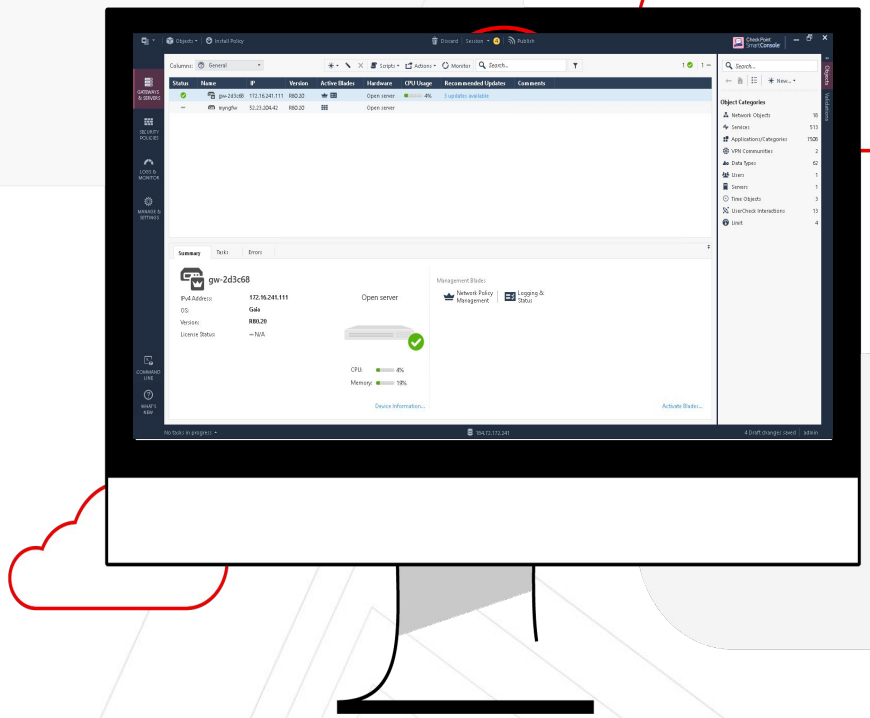
Managing Check Point Next Generation Firewalls

How do I use access Check Point firewalls?

- Accessed via a central management server
- Windows management software is called “SmartConsole”

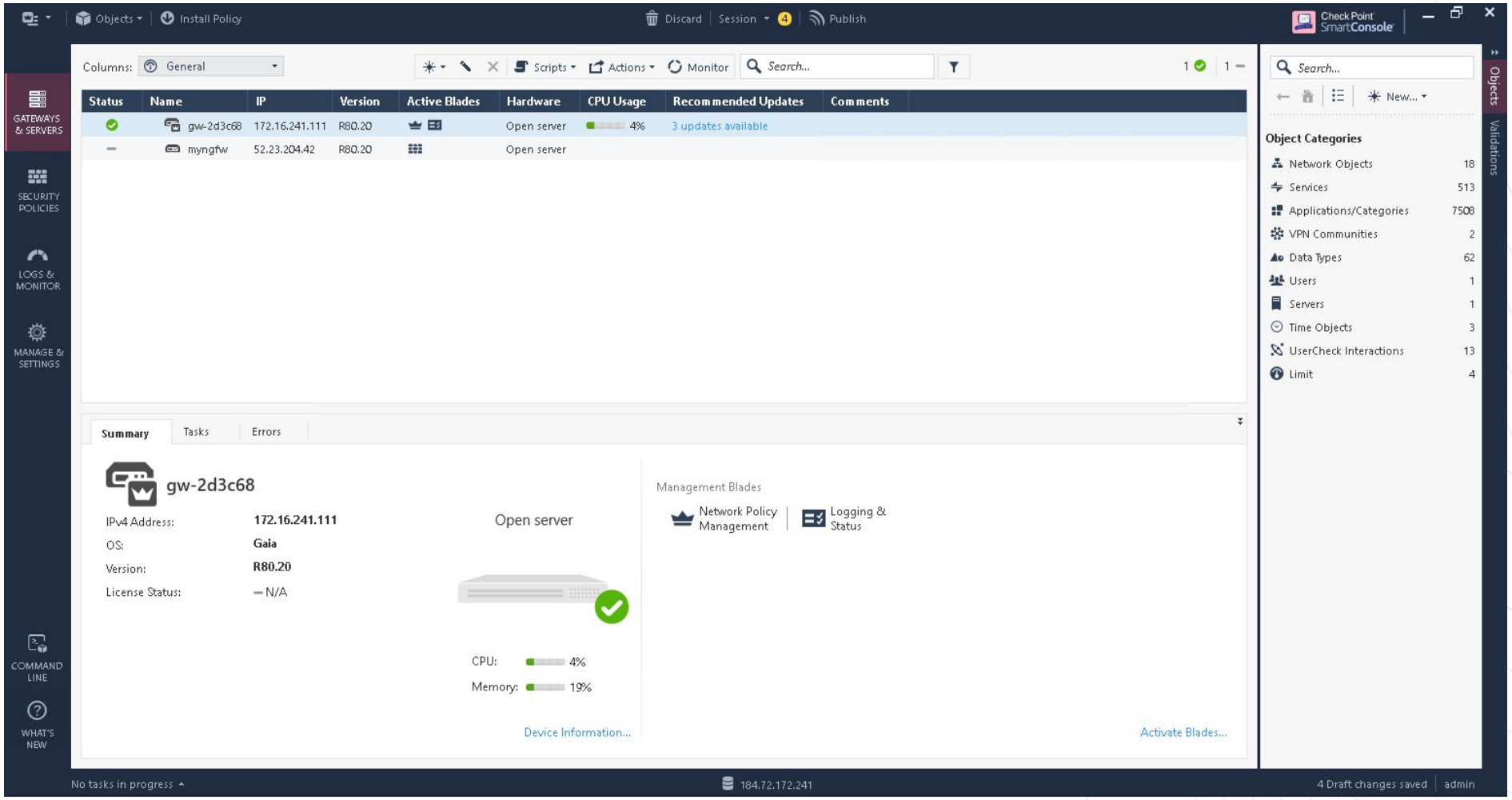
Lab Check Point instances?

- Lab SmartConsole instance is installed on your Windows host.
- Accessed via generic RDP client or lab-provided RDP-HTML5 client
- HTTP REST API used to call Check Point API



Red Hat

First Check Point Management Server Login



Red Hat

Ansible Playbook basics

Ansible playbooks

Playbook example

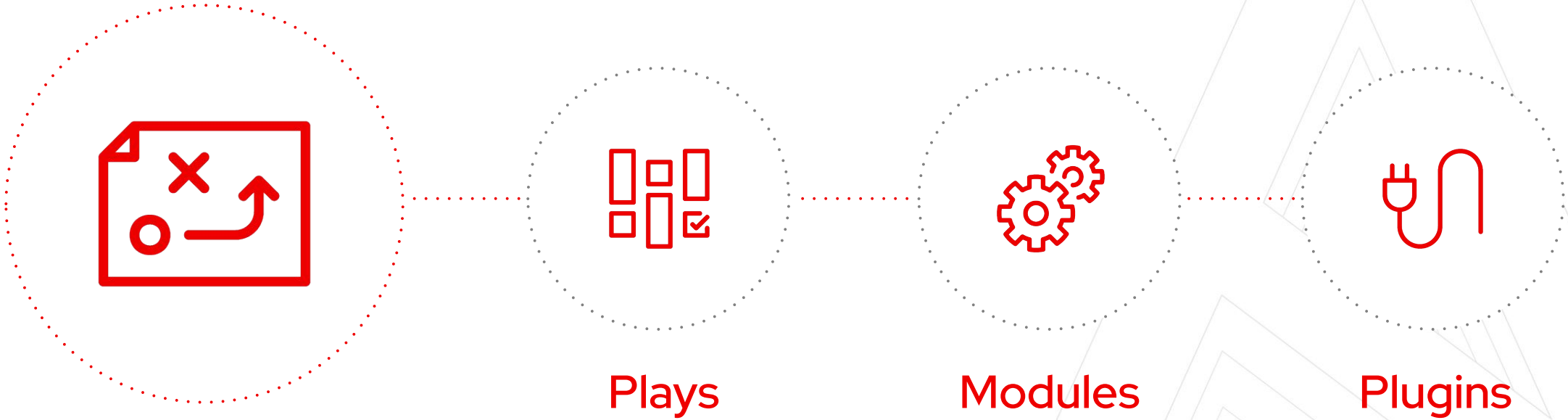
```
---
- name: install and start apache
  hosts: web
  become: yes

  tasks:
    - name: httpd package is present
      yum:
        name: httpd
        state: latest

    - name: latest index.html file is present
      template:
        src: files/index.html
        dest: /var/www/html/

    - name: httpd is started
      service:
        name: httpd
        state: started
```

What makes up an Ansible playbook?



Ansible plays

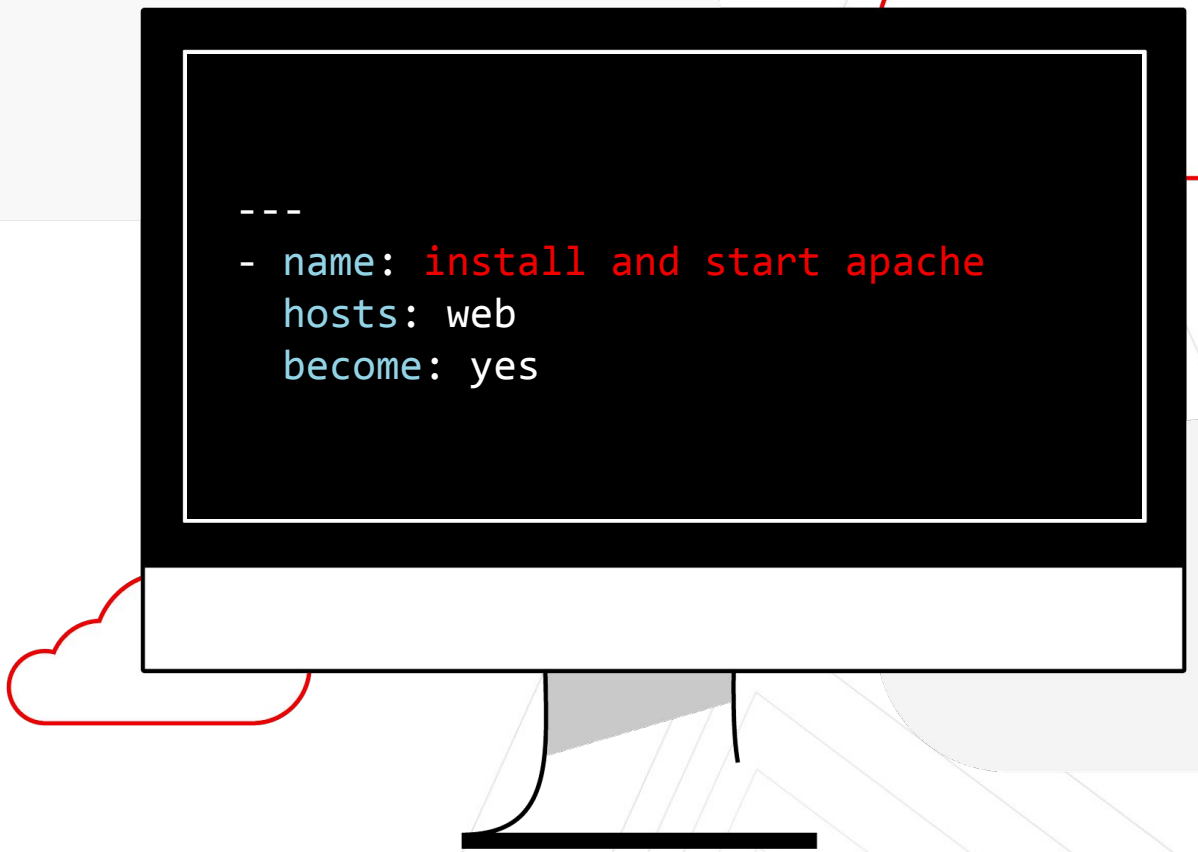
What am I automating?

What are they?

Top level specification for a group of tasks. Will tell that play which hosts it will execute on and control behavior such as fact gathering or privilege level.

Building blocks for playbooks

Multiple plays can exist within an Ansible playbook that execute on different hosts.



Ansible modules

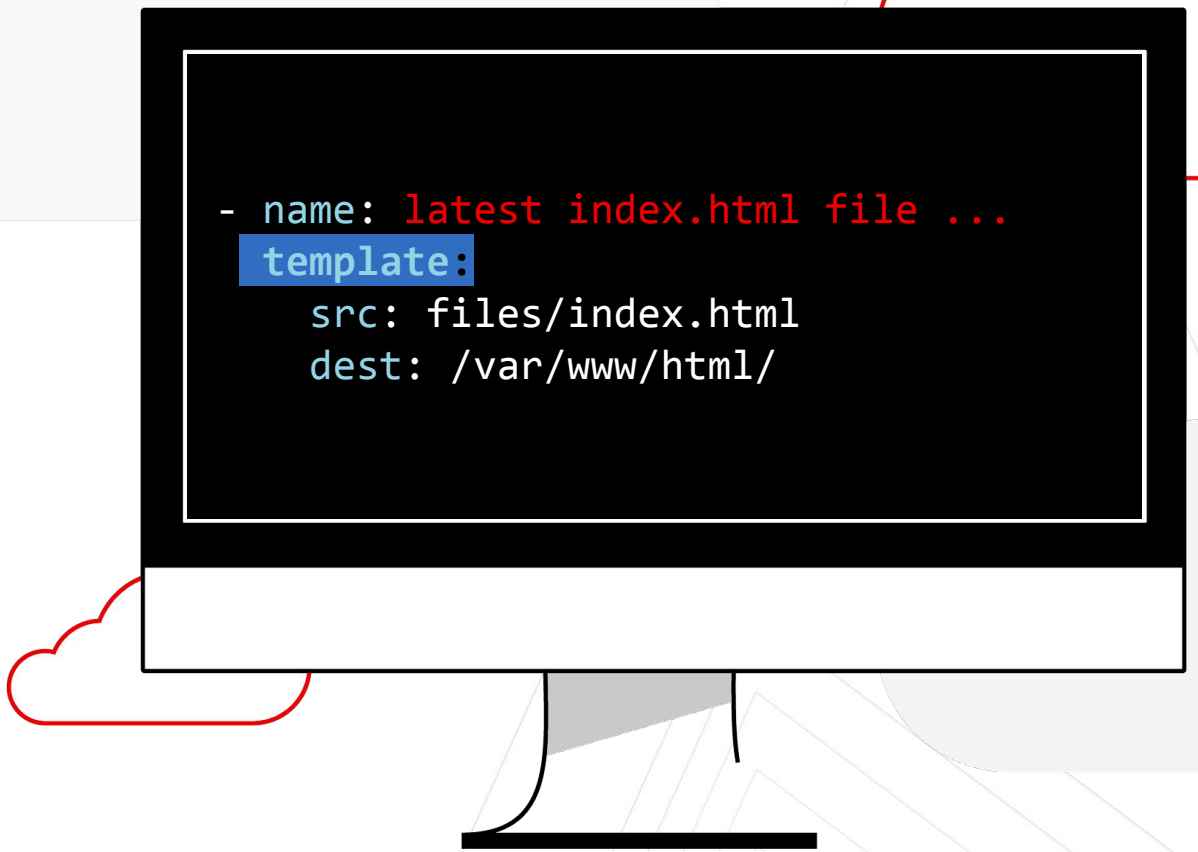
The “tools in the toolkit”

What are they?

Parametrized components with internal logic, representing a single step to be done.
The modules “do” things in Ansible.

Language

Usually Python, or Powershell for Windows setups. But can be of any language.



Ansible plugins

The “extra bits”

What are they?

Plugins are pieces of code that augment Ansible’s core functionality. Ansible uses a plugin architecture to enable a rich, flexible, and expandable feature set.

Example become plugin:

```
---
- name: install and start apache
  hosts: web
  become: yes
```

Example filter plugins:

```
{{ some_variable | to_nice_json }}
{{ some_variable | to_nice_yaml }}
```

Ansible playbooks

A play

```
---
- name: install and start apache
  hosts: web
  become: yes

  tasks:
    - name: httpd package is present
      yum:
        name: httpd
        state: latest

    - name: latest index.html file is present
      template:
        src: files/index.html
        dest: /var/www/html/

    - name: httpd is started
      service:
        name: httpd
        state: started
```

Ansible playbooks

A task

```
---
- name: install and start apache
  hosts: web
  become: yes

  tasks:
    - name: httpd package is present
      yum:
        name: httpd
        state: latest

    - name: latest index.html file is present
      template:
        src: files/index.html
        dest: /var/www/html/

    - name: httpd is started
      service:
        name: httpd
        state: started
```

Ansible playbooks

A module

```
---
- name: install and start apache
  hosts: web
  become: yes

  tasks:
    - name: httpd package is present
      yum:
        name: httpd
        state: latest

    - name: latest index.html file is present
      template:
        src: files/index.html
        dest: /var/www/html/

    - name: httpd is started
      service:
        name: httpd
        state: started
```

Ansible Colors

Running Playbooks

The most important colors of Ansible

```
A task executed as expected, no change was made.

A task executed as expected, making a change

A task failed to execute successfully
```

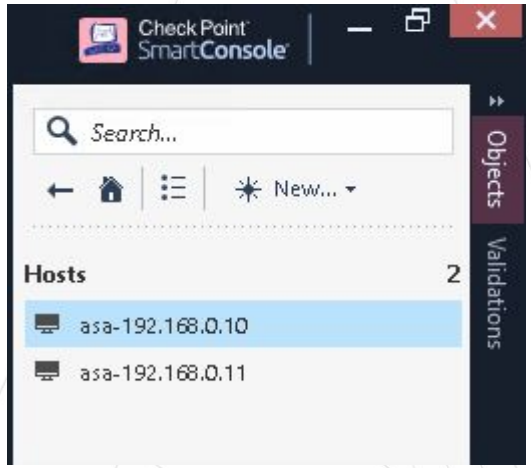
Running your first Playbook

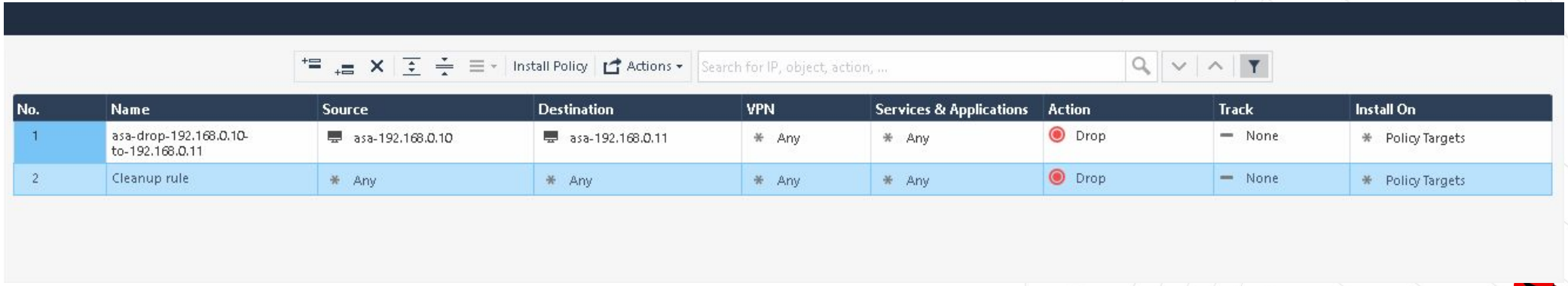
Verifying the playbook was successful

Check Point Firewall Policy

Log into SmartConsole

- Check Point Firewall Policy
- Check network objects for added hosts
- Check policies for added policy





Red Hat

Exercise Time!

Do Exercise 1.2 in your lab environment

- Follow the steps in the exercises
- Remember to use the IP addresses assigned to you
- The Check Point credentials differ from the standard workshop details provided.

Exercise 1.3

Topics Covered:

- What is an IDPS?
- Snort basics
- Intro to Ansible Roles
- Running a playbook interacting with Snort

What is an IDPS?

Intrusion Detection and Prevention Systems

What do they do?

- Monitors systems and networks
- Generates logs for malicious activity or policy violations
- Attempts to stop incident
- Logs are collected centrally, typically to a SIEM
- Typically used by security operations

Snort basics

Snort

Open Source Intrusion Detection and Prevention System

What does Snort do?

- Real time traffic analysis and packet logging on IP networks
- Content search and matching
- Service running on possible targets

Your Snort workshop instance

- Snort is installed on a RHEL instance
- RHEL instance accessed via SSH
- Ansible uses SSH connection to automate Snort

Snort Rules

Open Source Intrusion Detection and Prevention System

What are Snort rules?

- Rules determine what traffic is collected
- Rules define next step for collected traffic

Want more details on Snort rules?

- Snort rule infographic

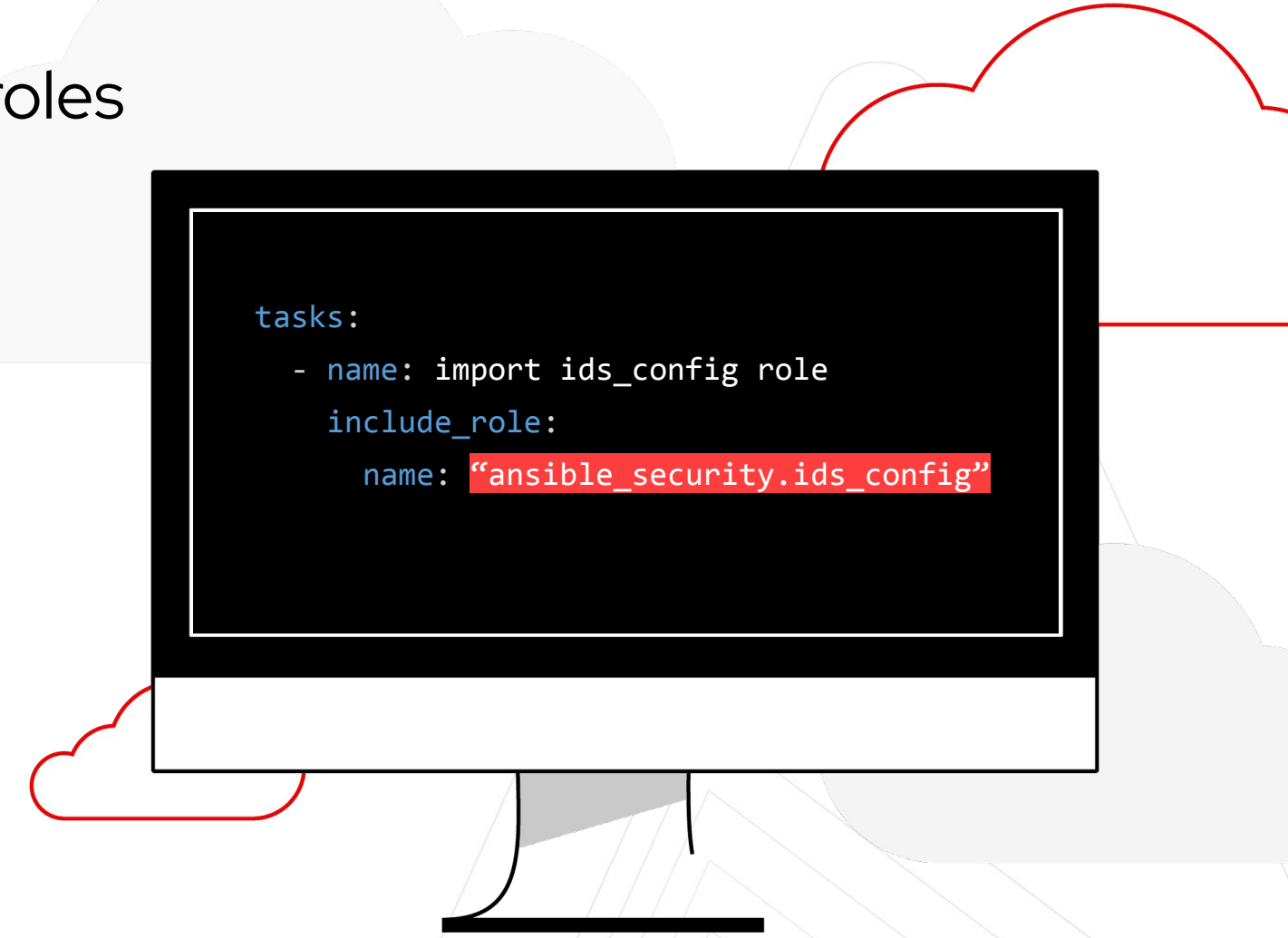
Intro to Ansible Roles

Ansible security automation roles

Reusable automation actions

What are Ansible roles?

- Group your tasks and variables of your automation in a reusable structure.
- Write roles once, and share them with others who have similar challenges in front of them.



Workshop Ansible Security Roles

- Already included in security EE
- `ids_config, ids_rule, log_manager`

Exercise Time!

Do Exercise 1.3 in your lab environment

- Follow the steps in the exercises
- Remember to use the IP addresses assigned to you

Exercise 1.4

Topics Covered:

- Intro to Automation Content Collections
- What is a SIEM?
- Introducing QRadar
- Automating your QRadar instance

Intro to Automation Content Collections

Ansible Content Collections

Simplified and consistent content delivery

What are they?

Collections are a data structure containing automation content:

- Modules, playbooks, roles, plugins, docs, tests

Workshop Ansible security collections

- Already included in security EE
- `ibm.qradar`, `ansible.security`, `check_point.mgmt` and more

Using Collections

Collections

```
nginx_core
├── MANIFEST.json
├── playbooks
│   ├── deploy-nginx.yml
│   └── ...
├── plugins
├── README.md
└── roles
    ├── nginx
    │   ├── defaults
    │   ├── files
    │   │   └── ...
    │   ├── tasks
    │   └── templates
    │       └── ...
    ├── nginx_app_protect
    └── nginx_config
```

deploy-nginx.yml

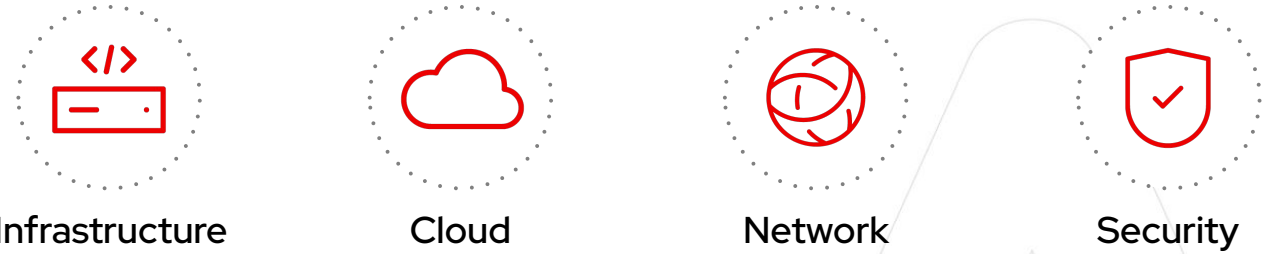
```yaml
---
- name: Install NGINX Plus
  hosts: all
  tasks:
    - name: Install NGINX
      include_role:
        name: nginxinc.nginx
      vars:
        nginx_type: plus

    - name: Install NGINX App Protect
      include_role:
        name: nginxinc.nginx_app_protect
      vars:
        nginx_app_protect_setup_license: false
        nginx_app_protect_remove_license: false
        nginx_app_protect_install_signatures: false
```

Certified Content Collections

90+

certified platforms



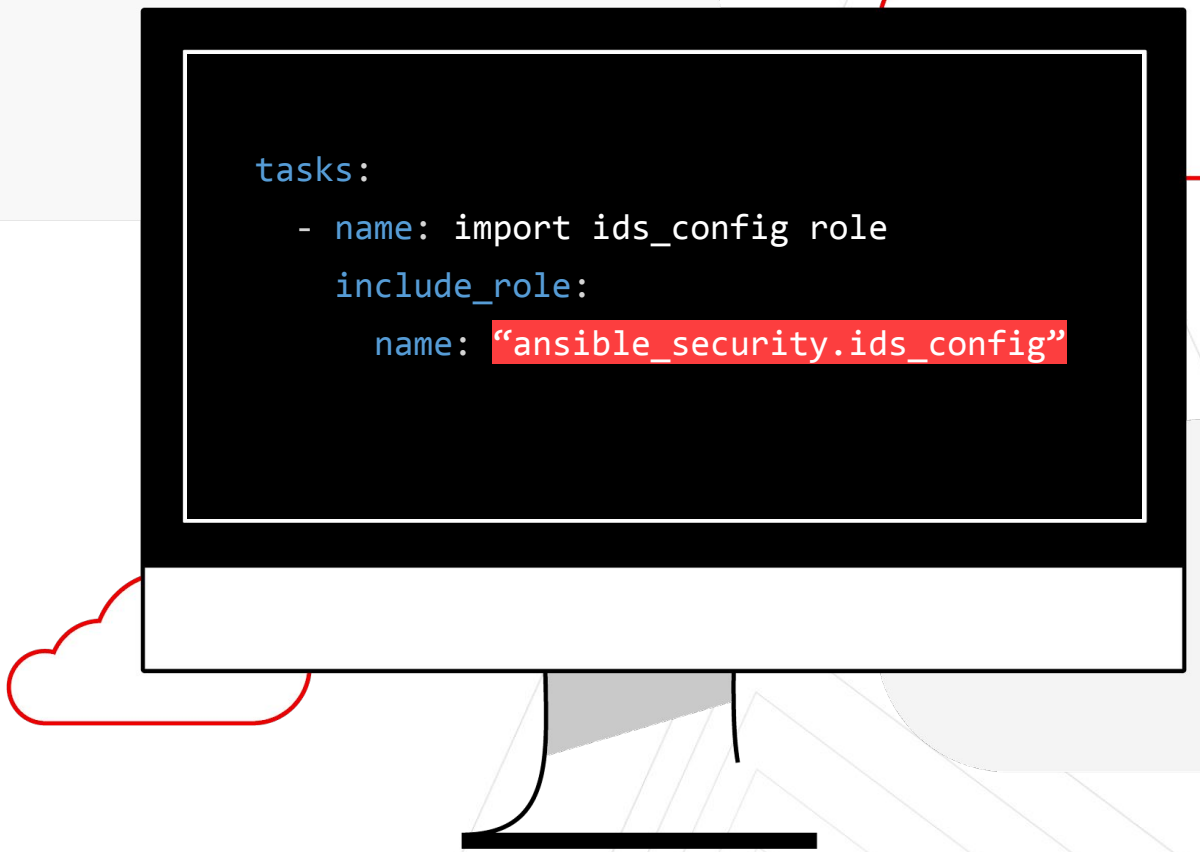
Red Hat
aws
ARISTA
Check Point
SOFTWARE TECHNOLOGIES LTD
NetApp
Google
CISCO
CYBERARK
IBM
Microsoft
f5
FORTINET

Ansible security automation Content Collections

Reusable automation actions

What are Ansible roles?

- Group your tasks and variables of your automation in a reusable structure.
- Write roles once, and share them with others who have similar challenges in front of them.



Workshop Ansible Security Roles

- Already included in security EE
- `ids_config, ids_rule, log_manager`

SIEM Overview

What is a SIEM?

Security Information and Event Management

What do they do?

- Supports threat detection, security incident management
- Real-time analysis of security alerts
- Aggregates activity from multiple sources
- Mostly used by security analysts

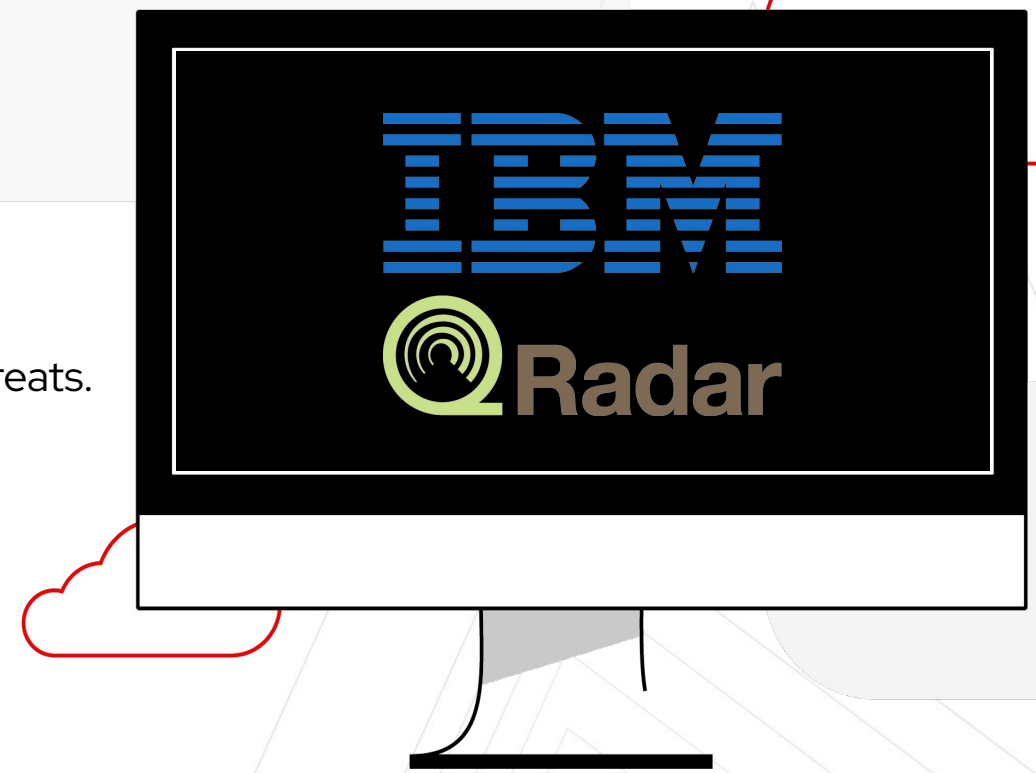
Introducing QRadar

IBM QRadar SIEM

Security and Information and Event Management

What does it do?

- Collects, analyses and stores network data in real time.
- Provides real-time information and monitoring
- Creates alerts and offenses, and responses to network threats.



QRadar Workshop Instance

- Uses `ibm.qradar` collection
- Ansible connects using QRadar HTTP API

IBM QRadar SIEM

Address most important security challenges

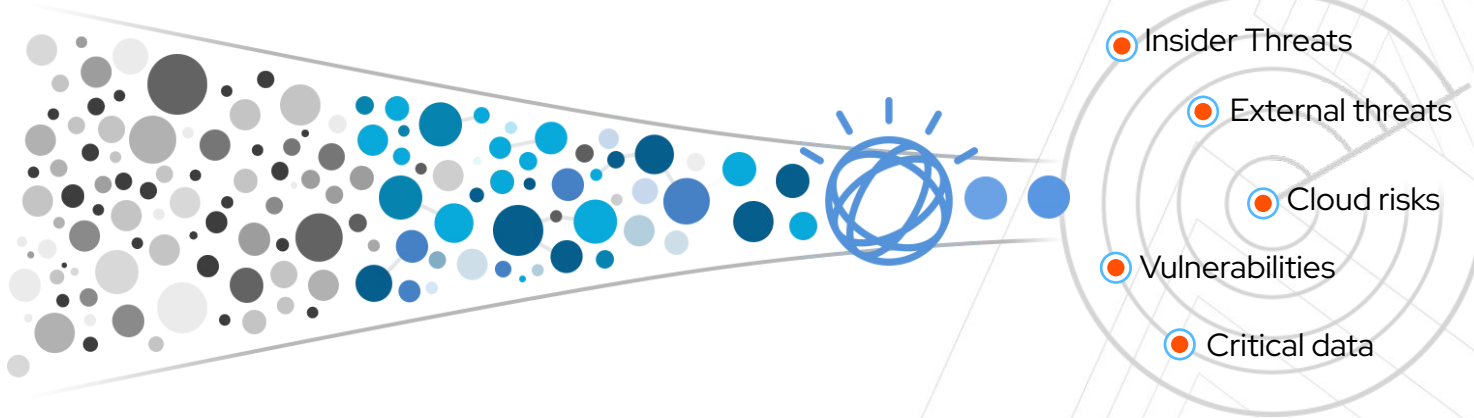
Complete Visibility

Endpoints
Network activity
Data activity
Users and identities
Threat intelligence
Configuration information
Vulnerabilities and threats
Application activity
Cloud platforms

Prioritized Threats

Automated Investigations

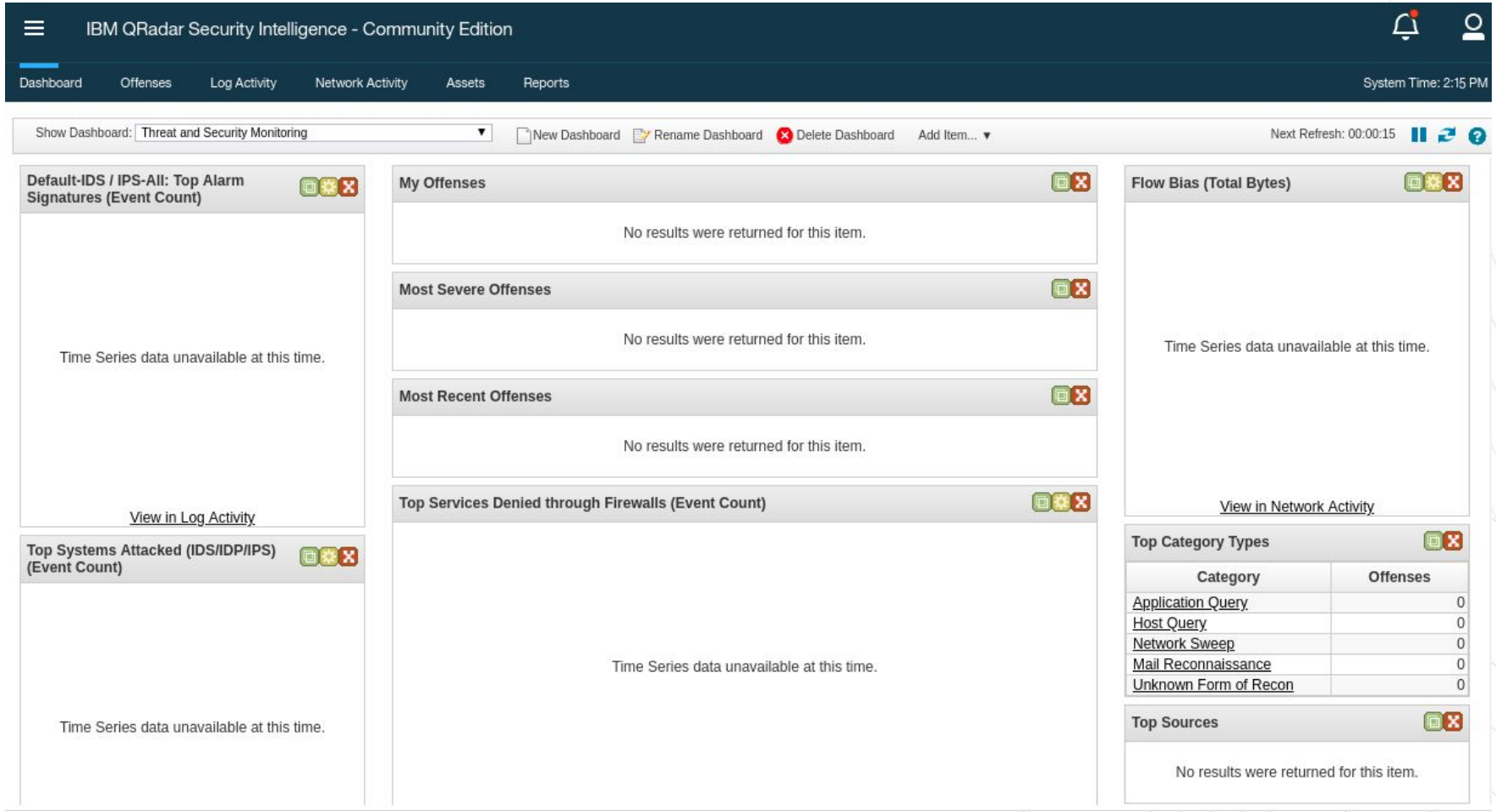
Proactive Hunting



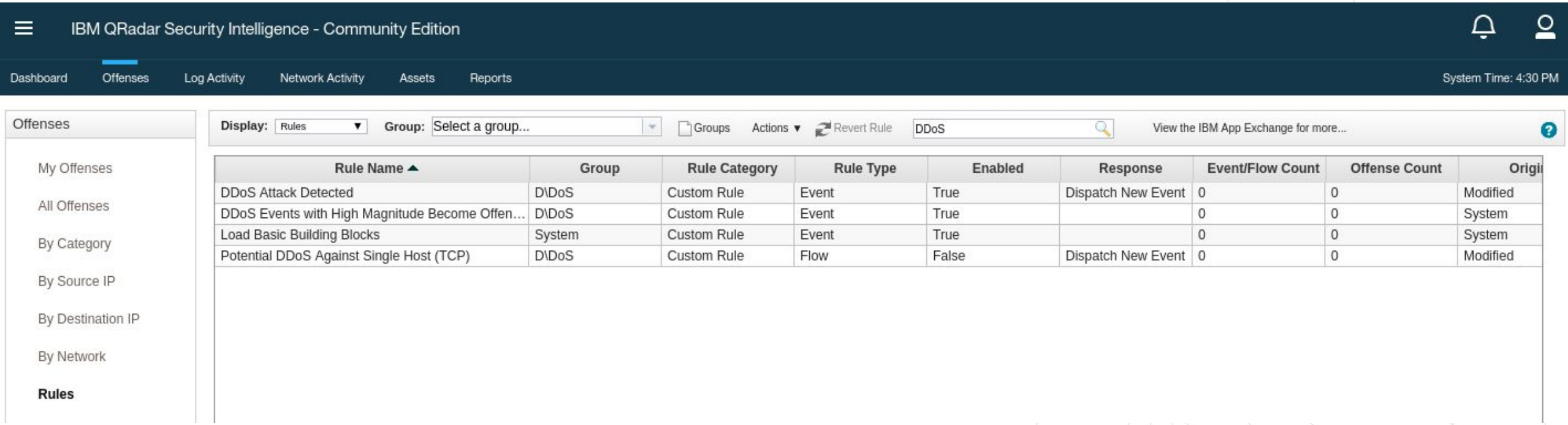
Red Hat

Automating your QRadar instance

IBM QRadar Interface



Verify Changes in the UI



Exercise Time!

Do Exercise 1.4 in your lab environment

- Follow the steps in the exercises
- Remember to use the IP addresses assigned to you
- QRadar credentials differ from the standard workshop username and password

Section 2

Security personas

Ansible Security Automation Use-Cases

Security Personas Overview

Security Personas

Security Operator

Toolset

- Firewalls, PAM, IDPS

Tasks

- Manage, configure security devices
- Escalate security events to analyst

Challenges

- Attacks more frequent and sophisticated

Security Analyst

Toolset

- SIEM, SOAR

Tasks

- Analyze and coordinate remediation

Challenges

- Attacks more frequent and sophisticated

Chief Information Security Officer

Resources

- Conferences, papers, analyst reports

Tasks

- Oversee security operations
- Direct and manage security strategy

Challenges

- Multiple, siloed security teams

Red Hat

Exercise 2.1

Topics Covered:

- What is investigation enrichment?
- Lab scenario overview

What is investigation enrichment?

Collate, investigate and build context for security anomalies

What is investigation enrichment?

- Process of adding contextual information to security events
- Vital for effective security response
- Typically performed by security analyst
- Events redirected to a SIEM

Lab Scenario

- You, the security analyst, is informed of a security anomaly
- You need to gather events from devices and investigate the event

Investigation Enrichment Scenario overview

Investigation Enrichment

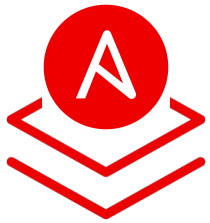
Attacker launches web attack

Investigation Enrichment

Anomaly detected

Analyst

SIEM



Ansible Automation Platform

1 Launches attack

Attacker

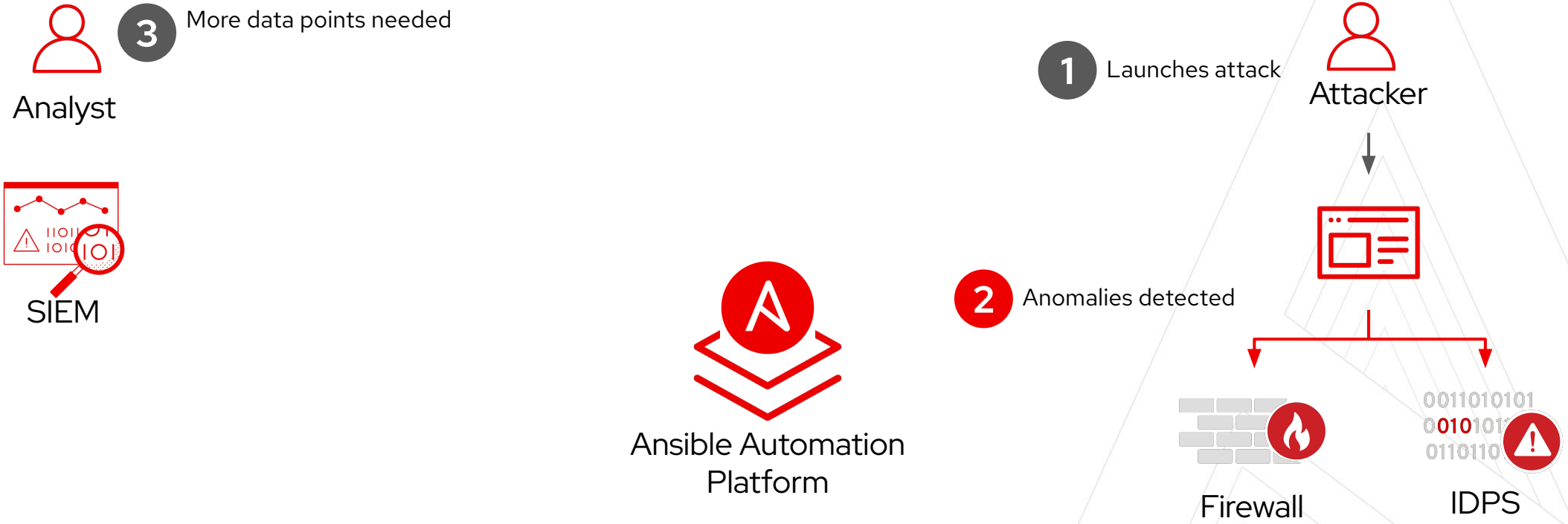
2 Anomalies detected

Firewall

IDPS

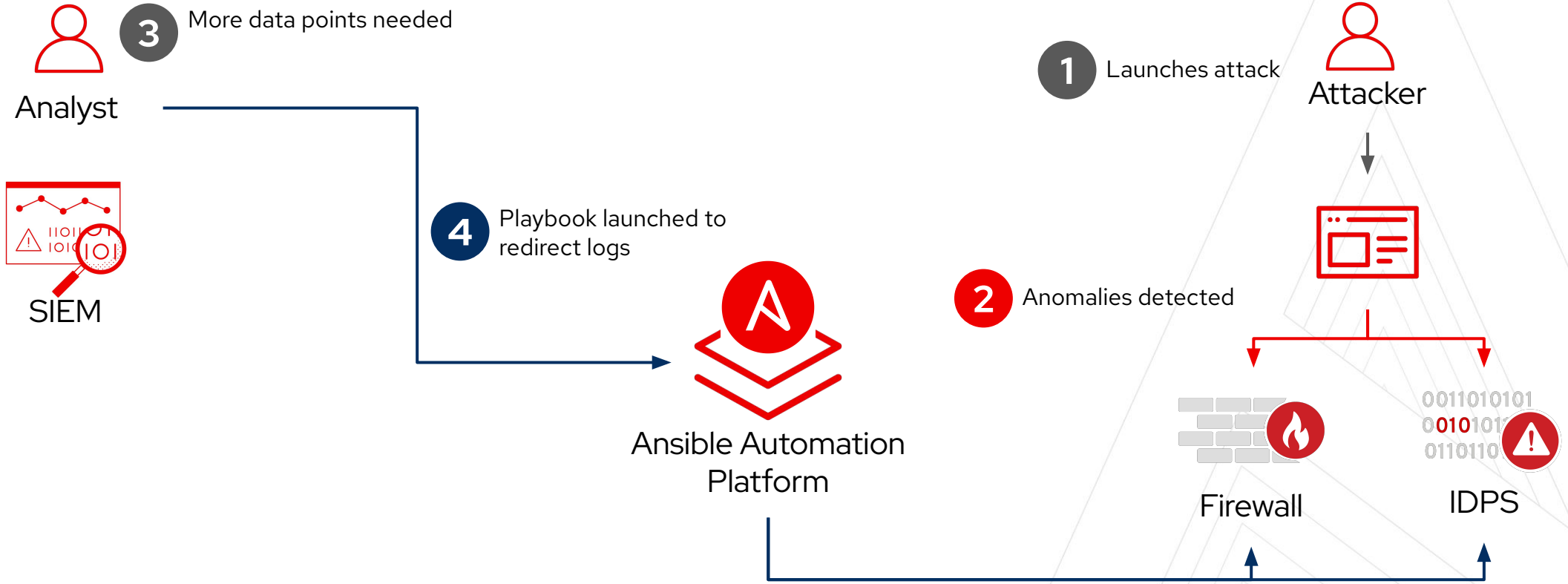
Investigation Enrichment

Analyst needs more data points to assess anomaly



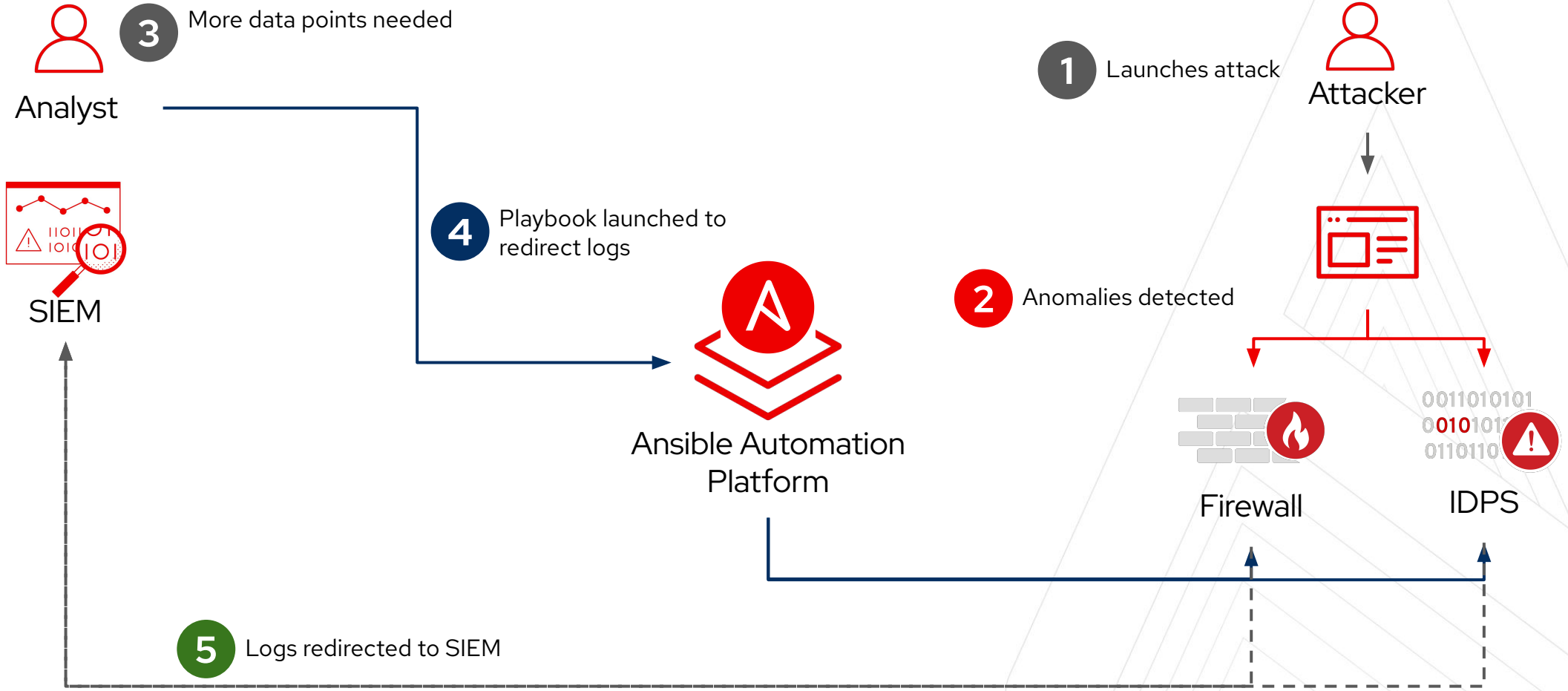
Investigation Enrichment

Playbook launched to redirect logs to SIEM for analysis



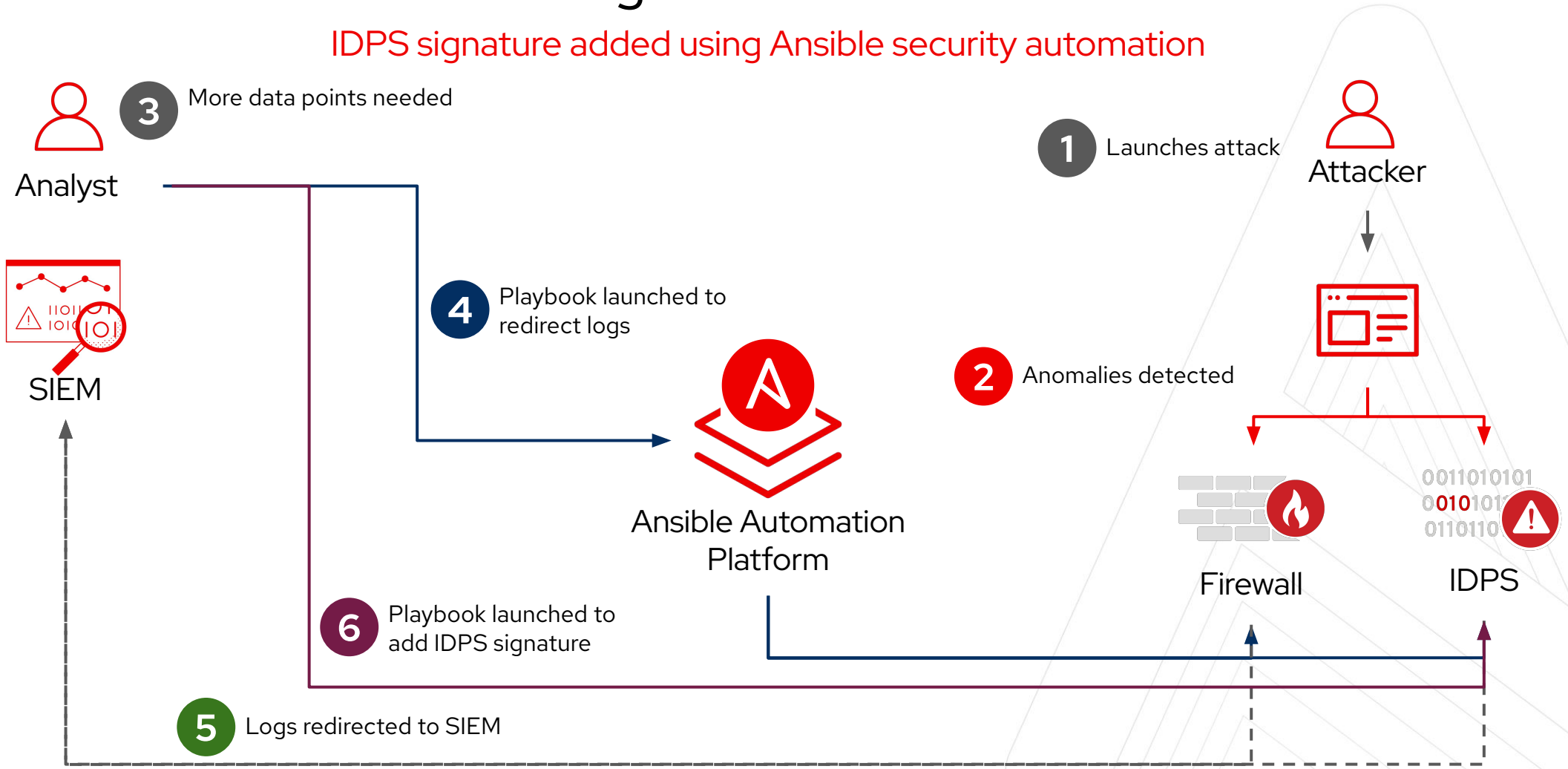
Investigation Enrichment

Ansible security automation redirects events to SIEM



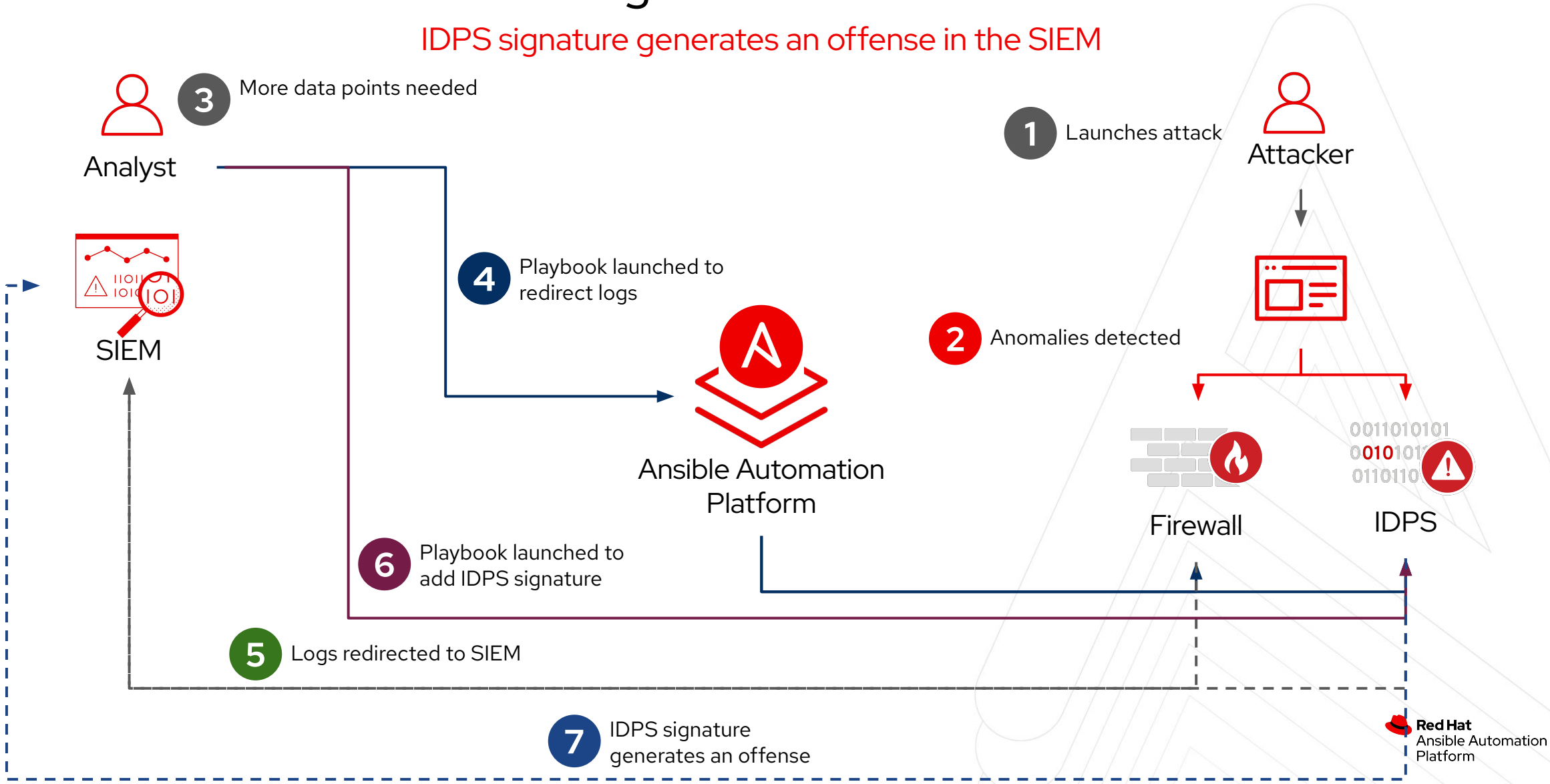
Investigation Enrichment

IDPS signature added using Ansible security automation



Investigation Enrichment

IDPS signature generates an offense in the SIEM



Exercise Time!

Do Exercise 2.1 in your lab environment

- Follow the steps in the exercises
- Remember to use the IP addresses assigned to you

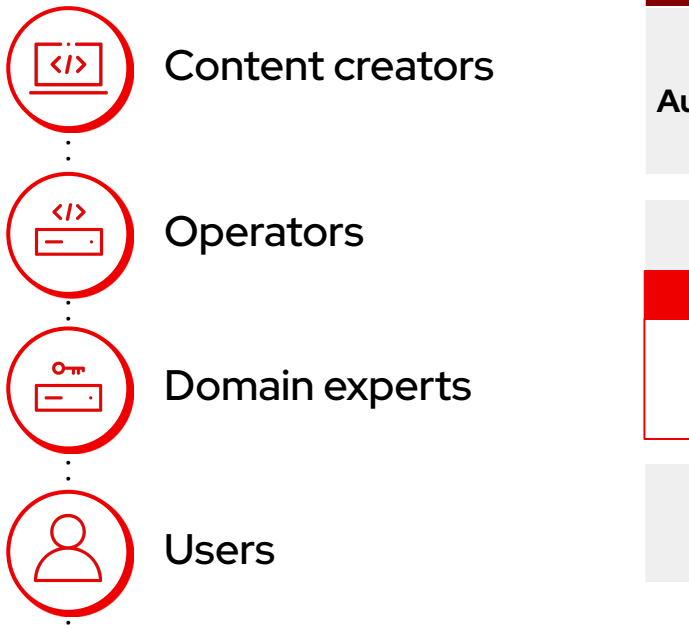
Exercise 2.2

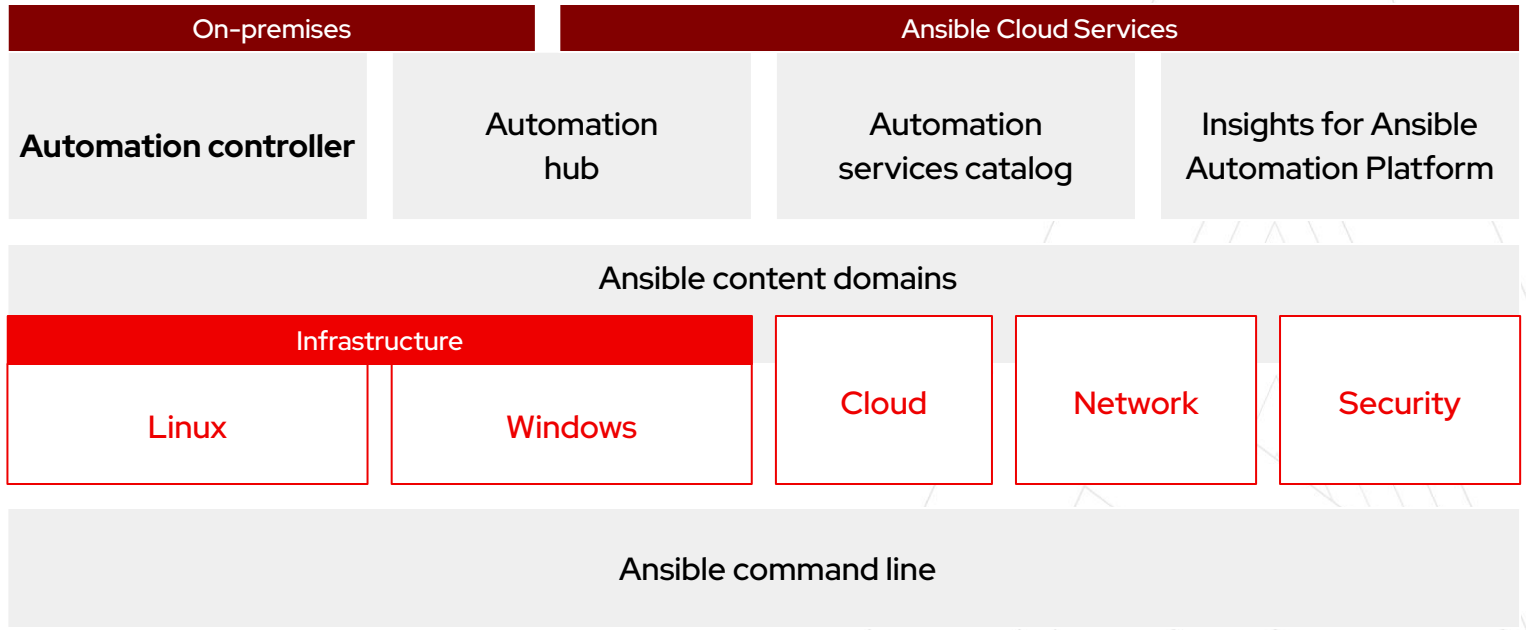
Topics Covered:

- Introduction to automation controller
- What is threat hunting?
- Lab scenario overview

Introduction to Automation controller

Red Hat Ansible Automation Platform





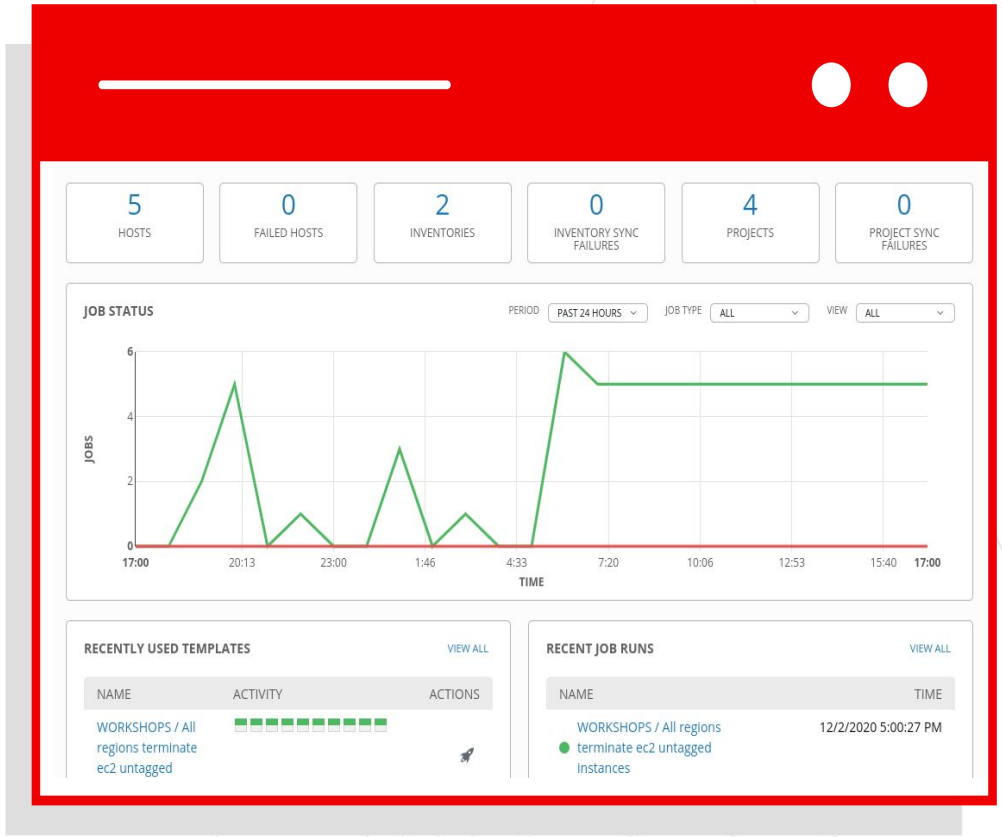
Fueled by an open source community

What is Automation controller?

Automation controller is a UI and RESTful API allowing you to scale IT automation, manage complex deployments and speed productivity.

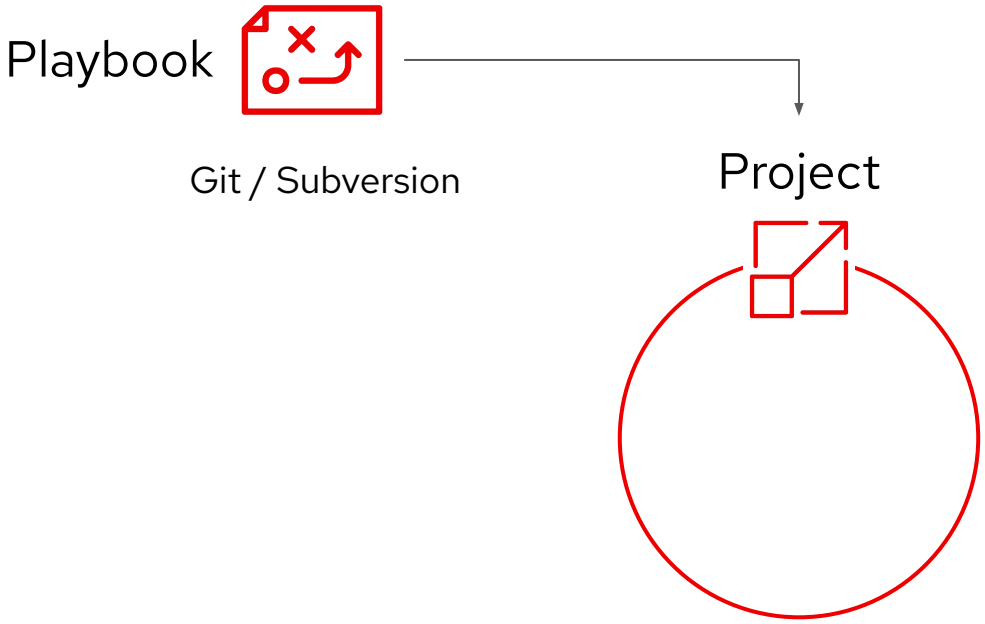
Automation controller provides

- Role-based access control
- Push-button deployment access
- All automations are centrally logged
- Powerful workflows match your IT processes

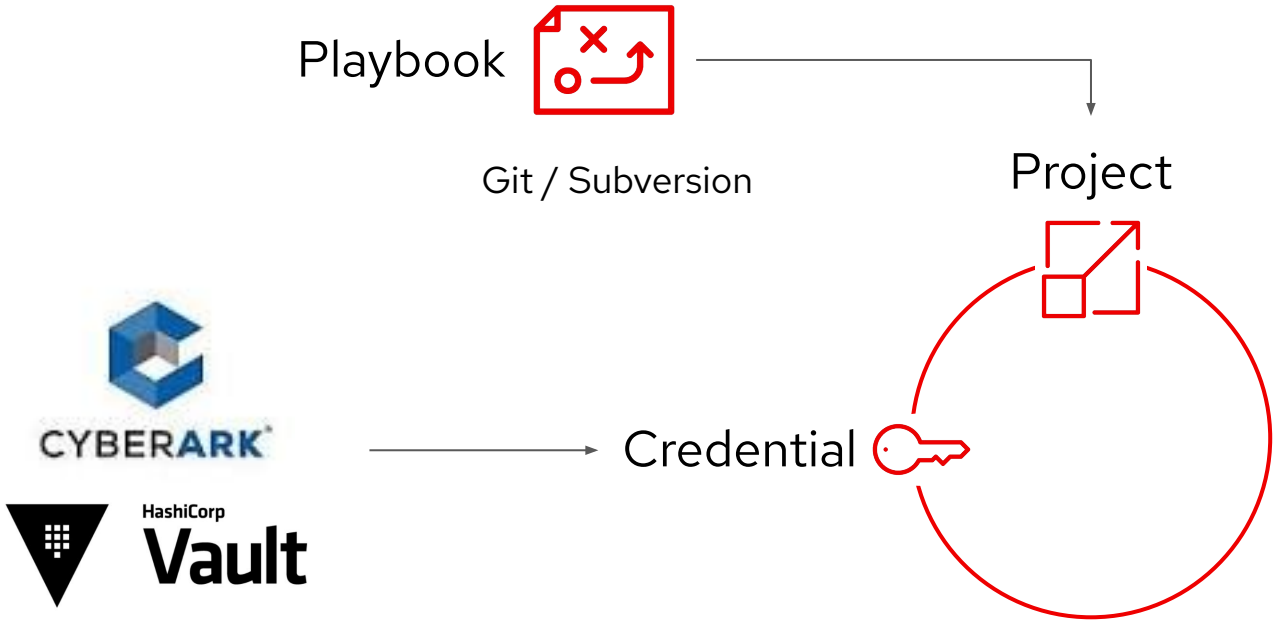


Red Hat
Ansible Automation
Platform

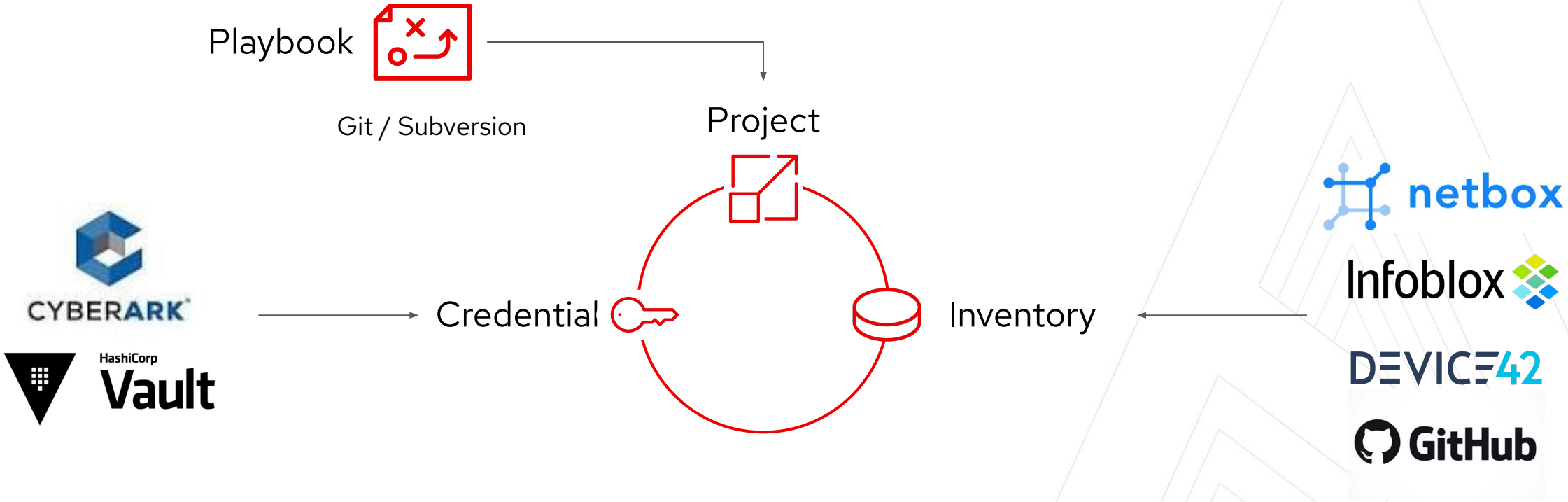
Anatomy of an Automation Job



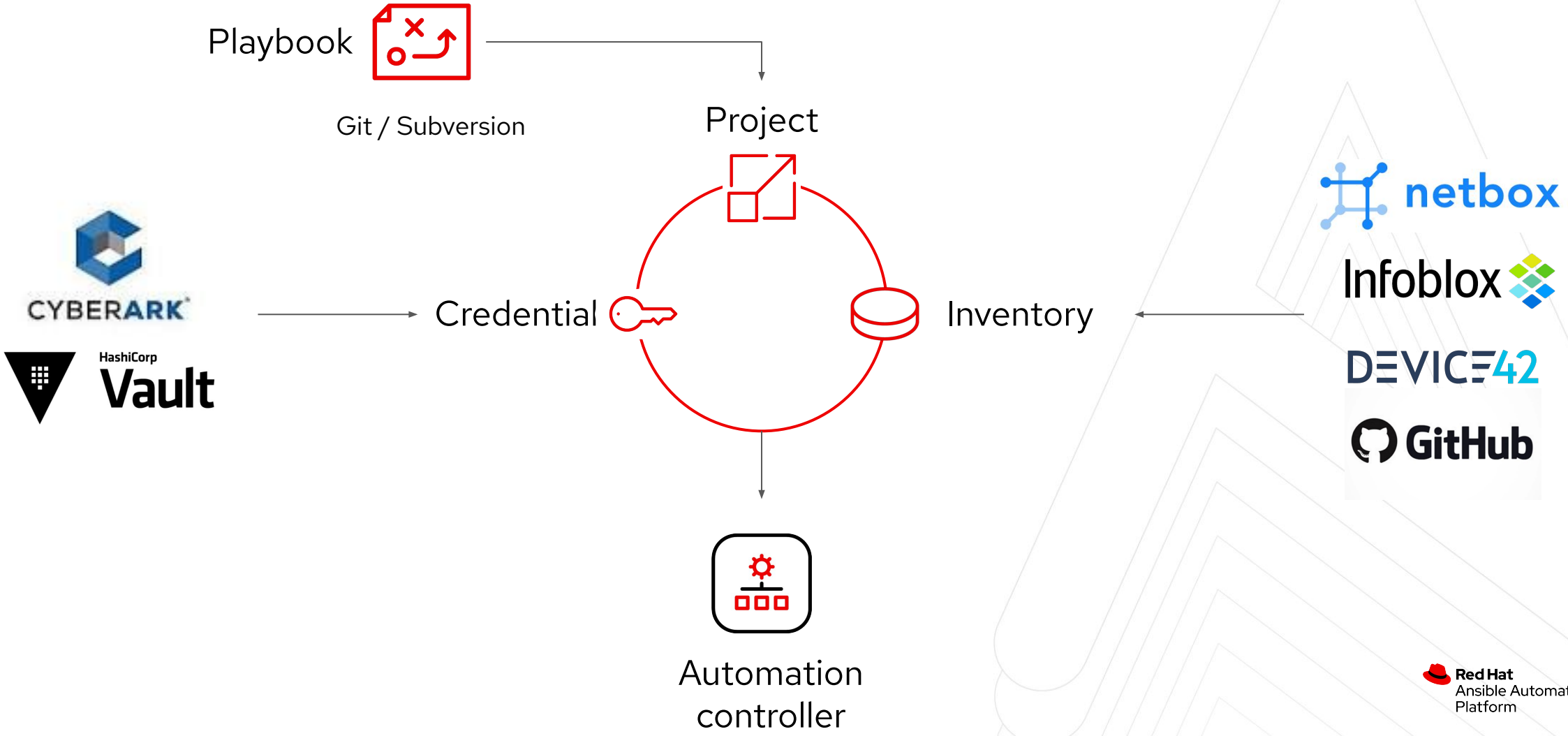
Anatomy of an Automation Job



Anatomy of an Automation Job



Anatomy of an Automation Job

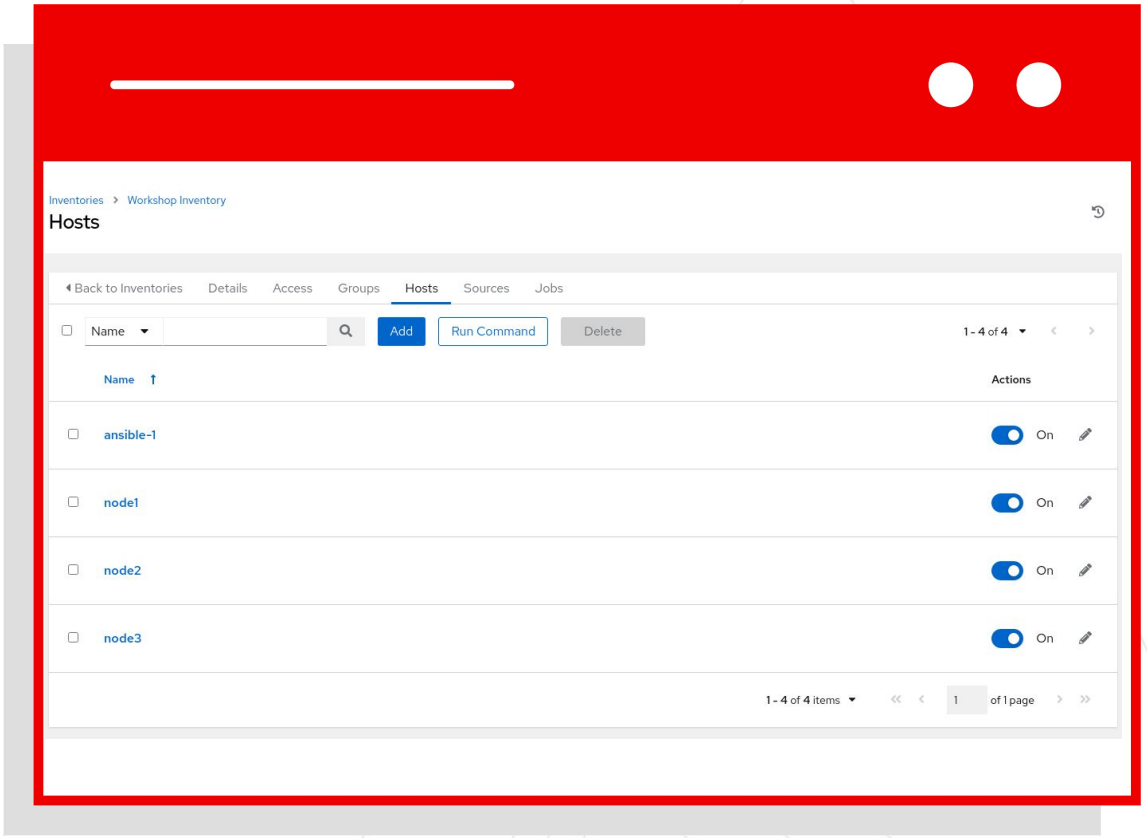


Automation controller features

Inventories

Inventory is a collection of hosts (nodes) with associated data and groupings that Automation Controller can connect to and manage.

- Hosts (nodes)
- Groups
- Inventory-specific data (variables)
- Static or dynamic sources

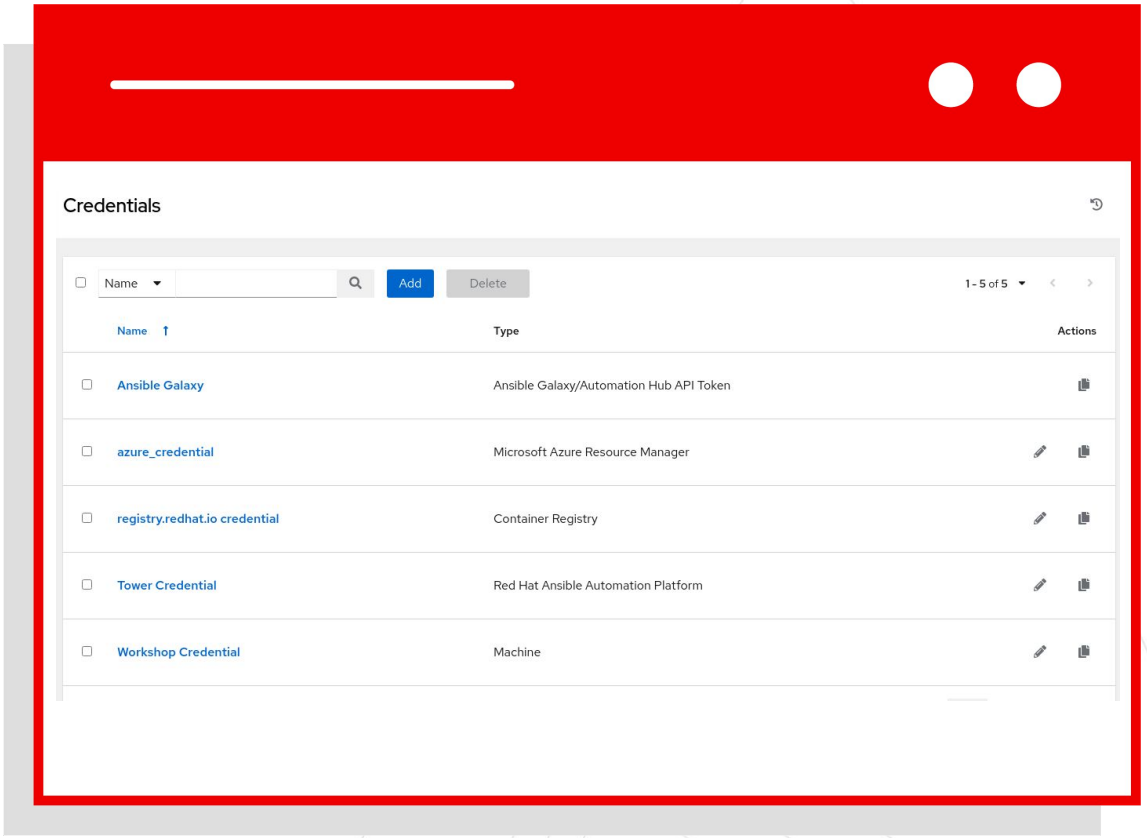


Credentials

Credentials are utilized by Automation Controller for authentication with various external resources:

- Connecting to remote machines to run jobs
- Syncing with inventory sources
- Importing project content from version control systems
- Connecting to and managing network devices

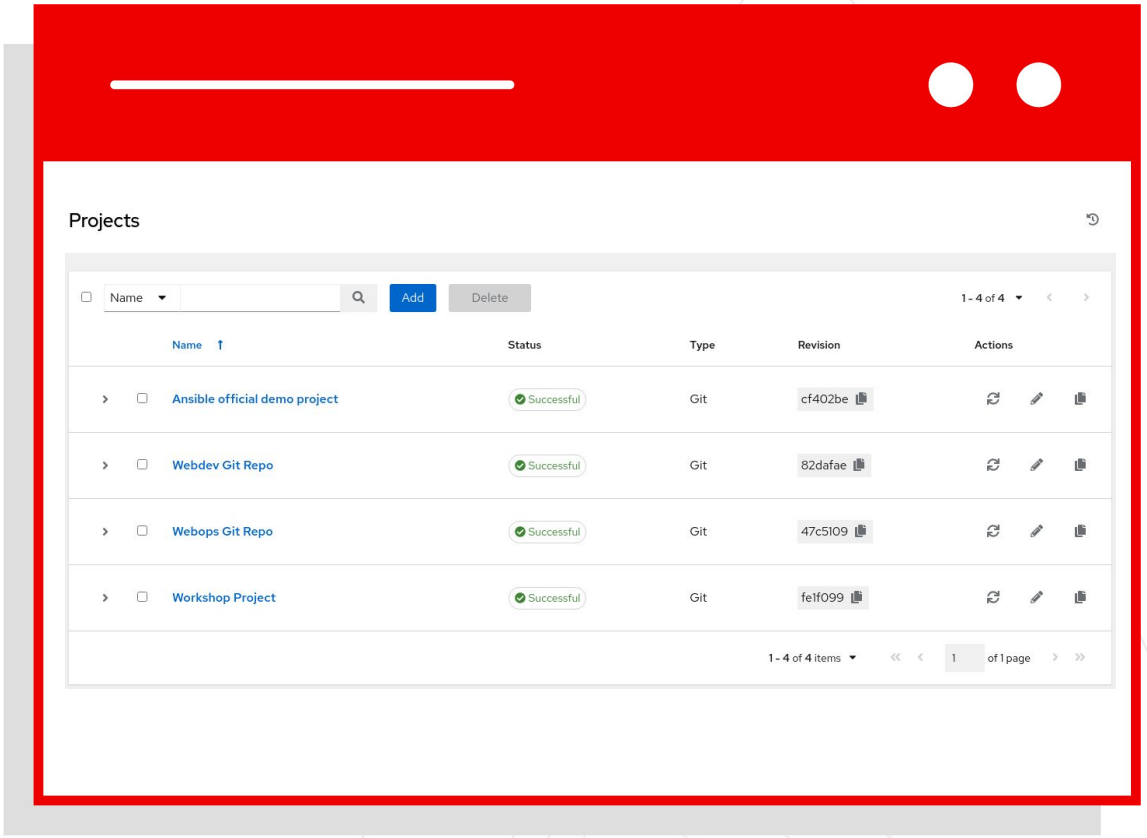
Centralized management of various credentials allows end users to leverage a secret without ever exposing that secret to them.



Project

A project is a logical collection of Ansible Playbooks, represented in Ansible Automation Controller.

You can manage Ansible Playbooks and playbook directories by placing them in a source code management system supported by automation controller, including Git, Subversion, and Mercurial.

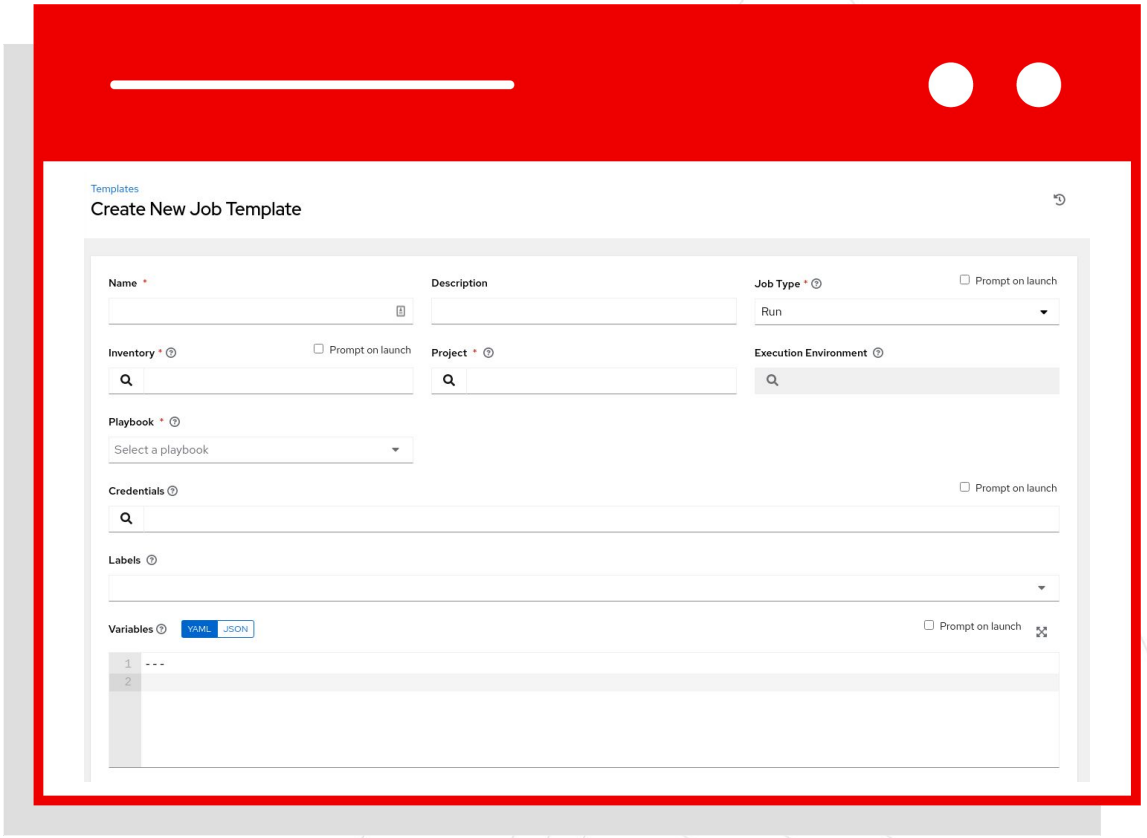


Job Templates

Everything in automation controller revolves around the concept of a **Job Template**. Job Templates allow Ansible Playbooks to be controlled, delegated and scaled for an organization.

A **Job Template** requires:

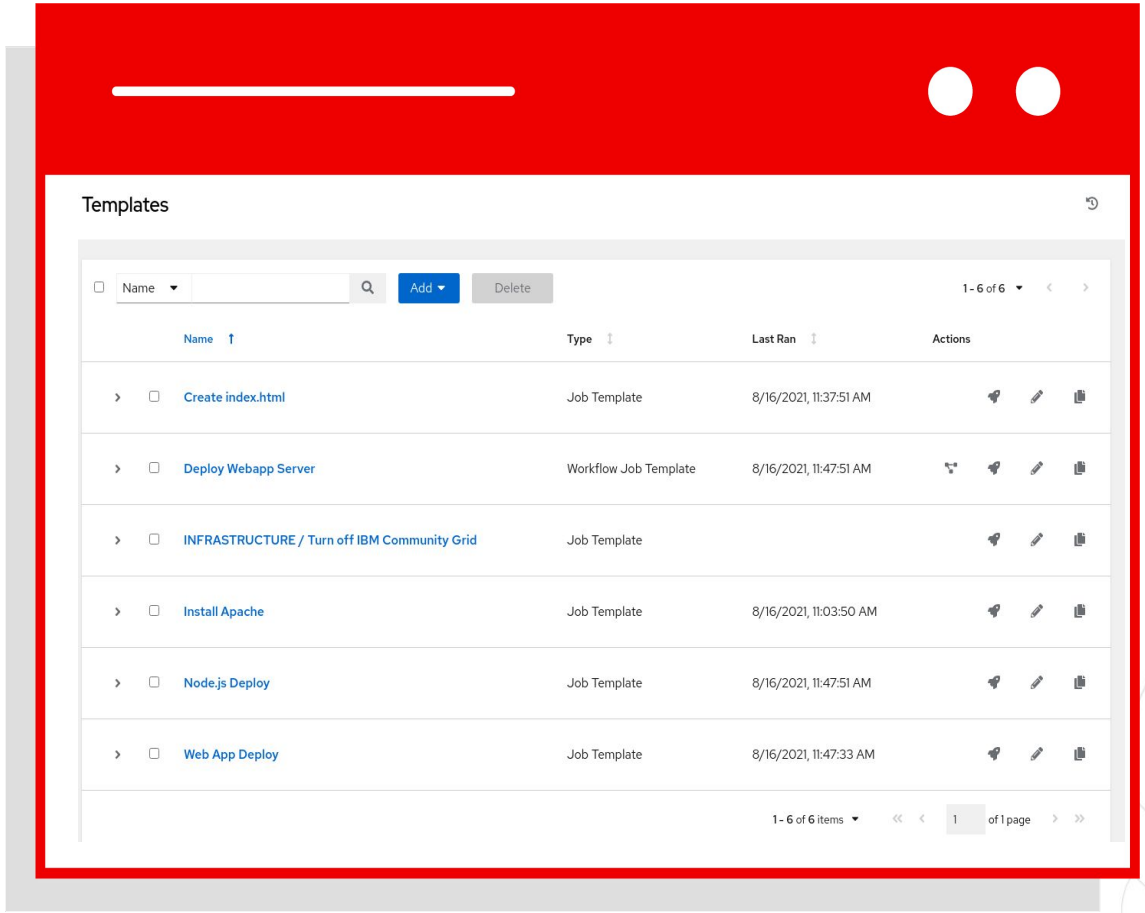
- An **Inventory** to run the job against
- A **Credential** to login to devices.
- A **Project** which contains Ansible Playbooks



Red Hat
Ansible Automation
Platform

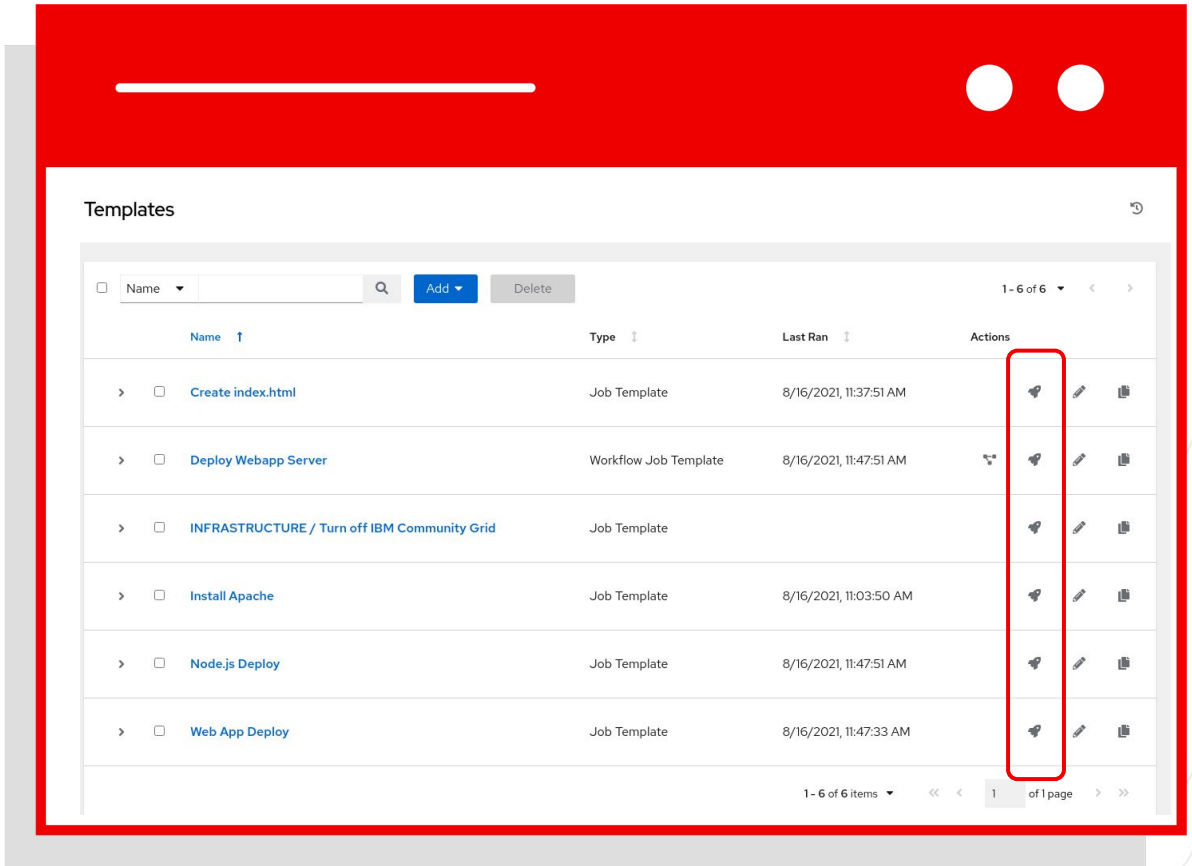
Expanding on Job Templates

Job Templates can be found and created by clicking the **Templates** button under the *Resources* section on the left menu.



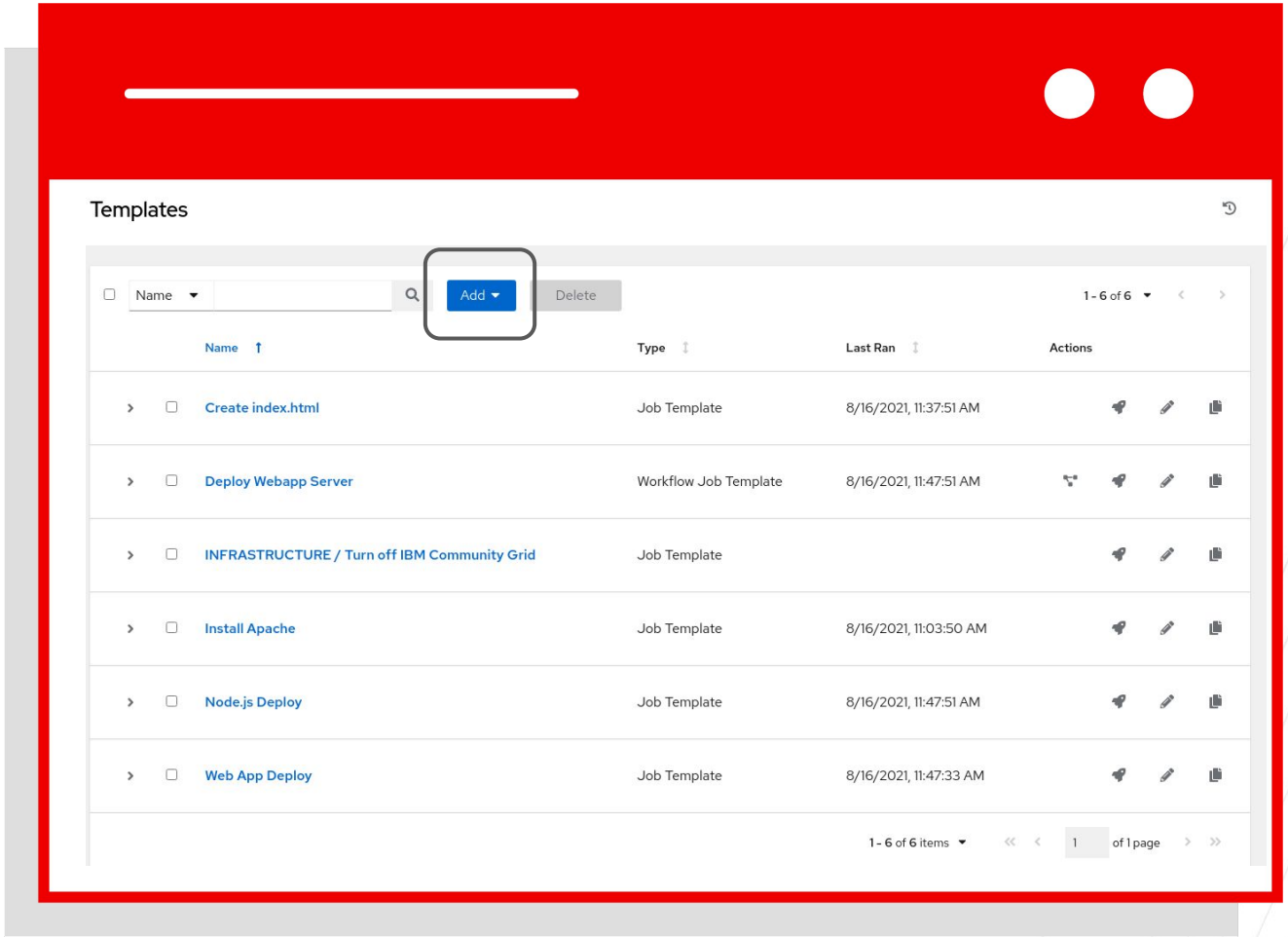
Executing an existing Job Template

Job Templates can be launched by clicking the **rocketship button** for the corresponding Job Template



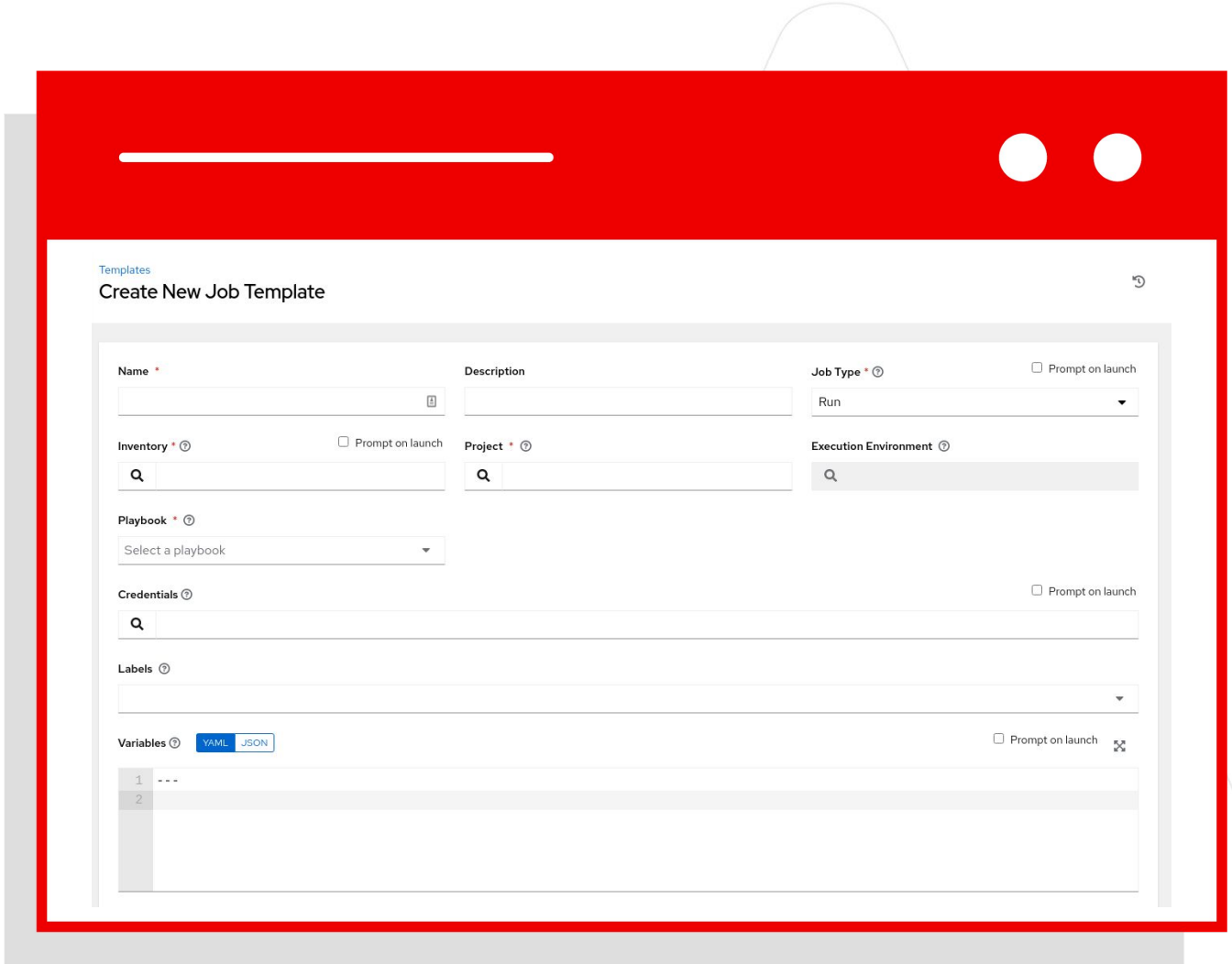
Creating a new Job Template (1/2)

New Job Templates can be created by clicking the **Add button**



Creating a new Job Template (2/2)

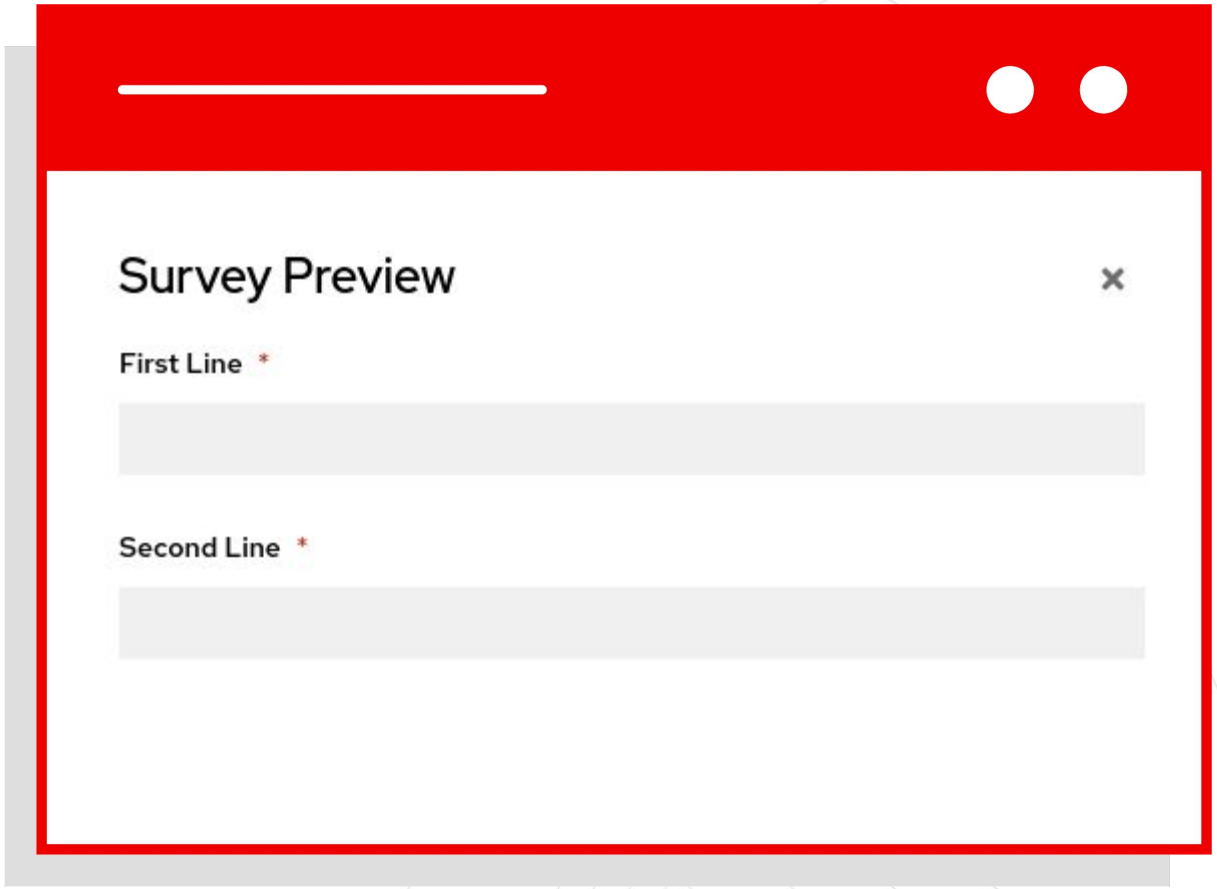
This **New Job Template** window is where the inventory, project and credential are assigned. The red asterisk * means the field is required .



Surveys

Controller surveys allow you to configure how a job runs via a series of questions, making it simple to customize your jobs in a user-friendly way.

An Automation controller survey is a simple question-and-answer form that allows users to customize their job runs. Combine that with controller's role-based access control, and you can build simple, easy self-service for your users.

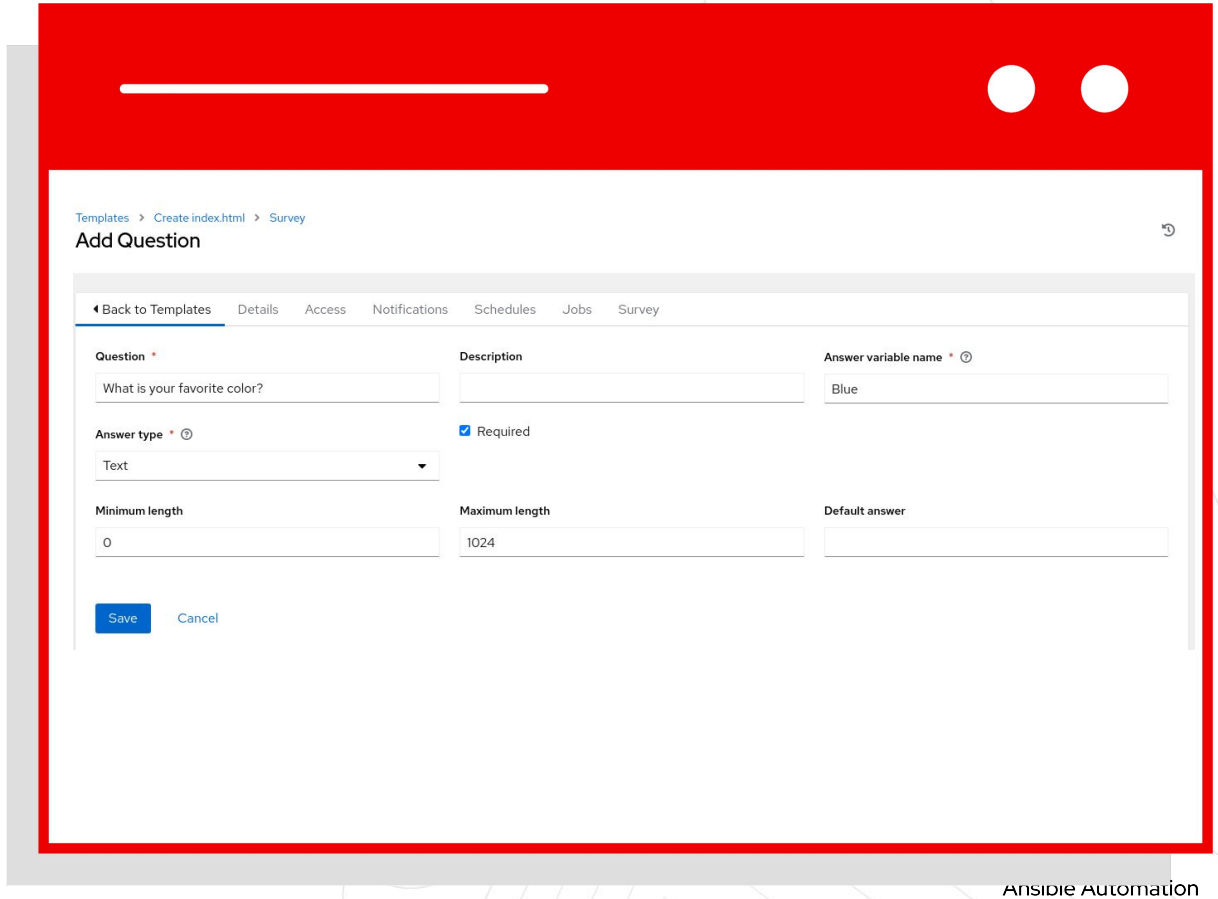


Creating a Survey (1/2)

Once a Job Template is saved, the Survey menu will have an **Add**

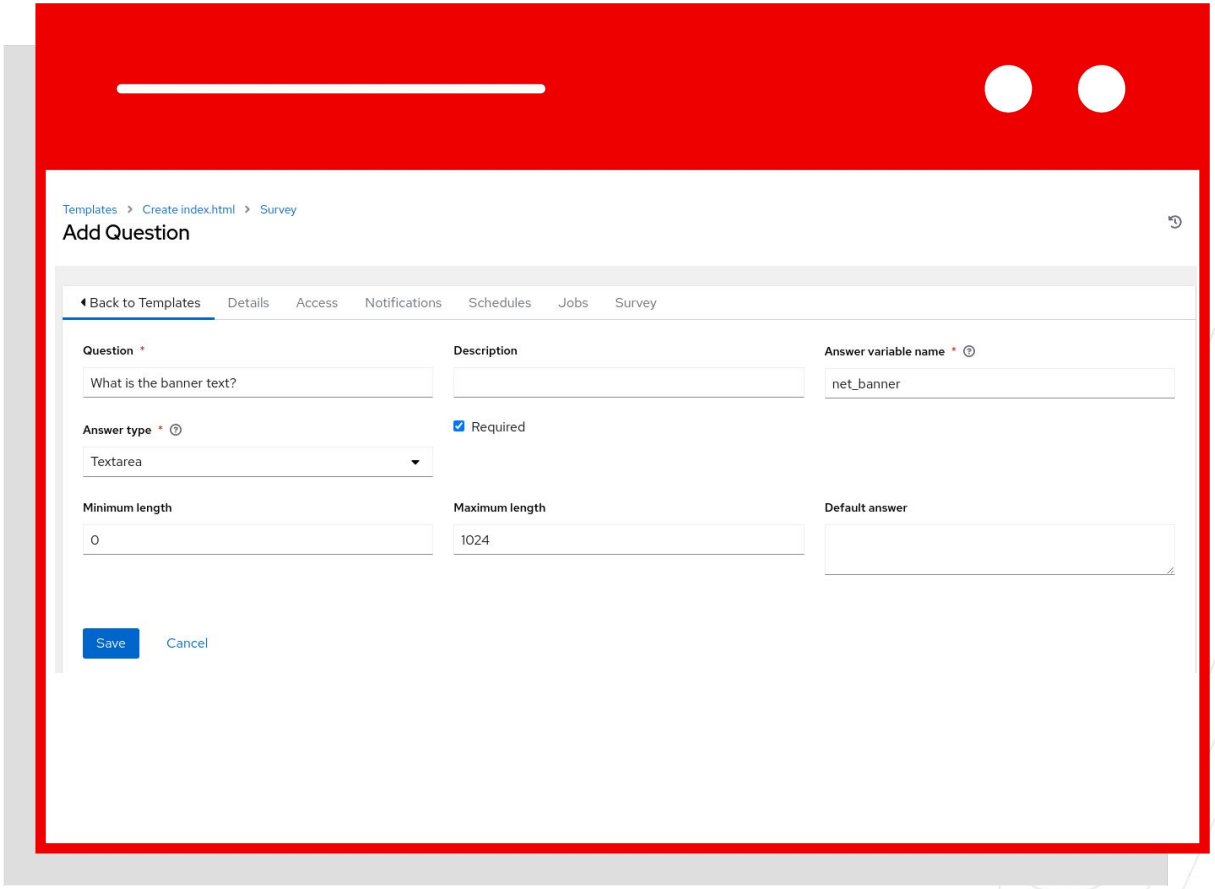
Button

Click the button to open the Add Survey window.



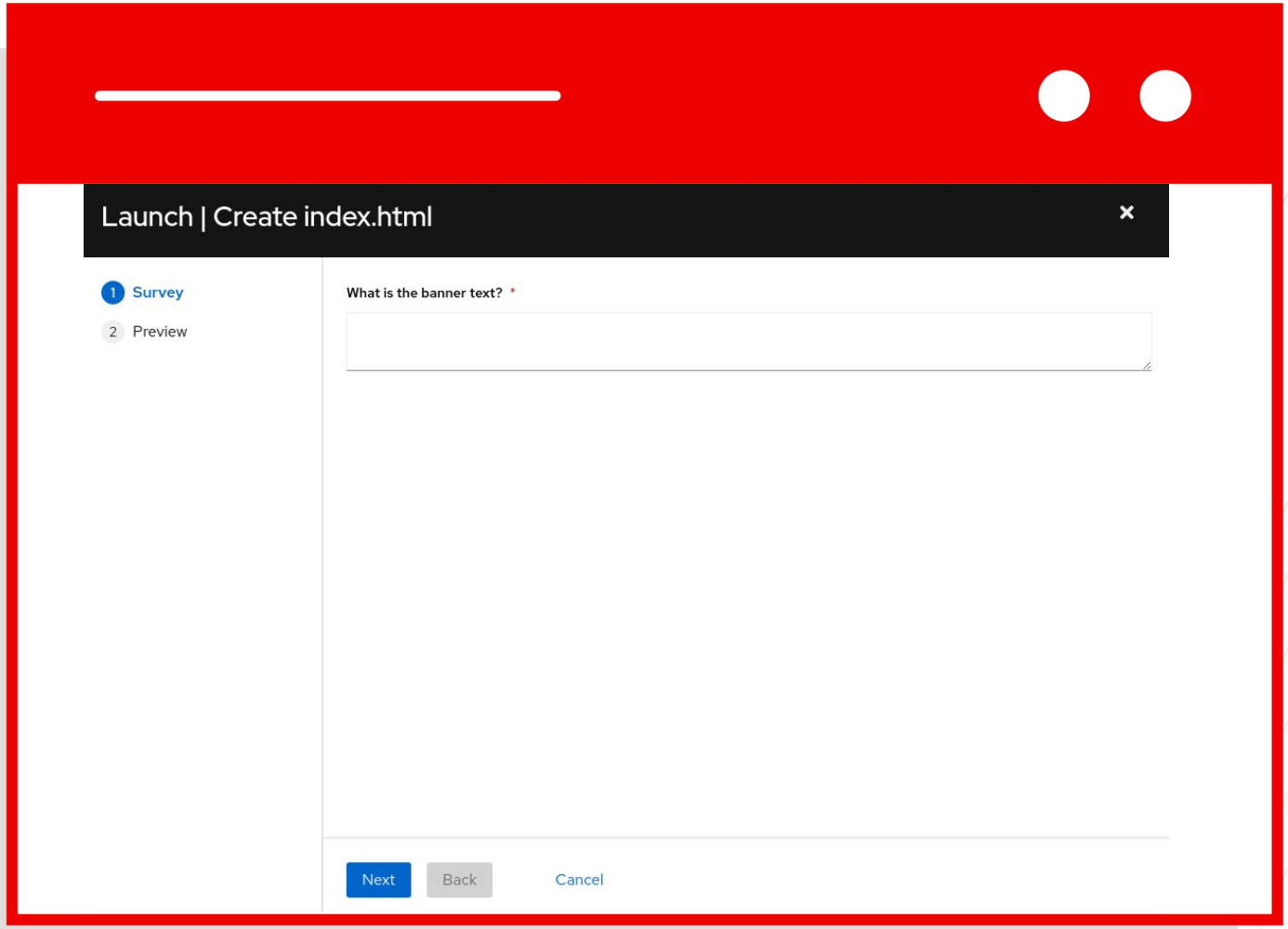
Creating a Survey (2/2)

The Add Survey window allows the Job Template to prompt users for one or more questions. The answers provided become variables for use in the Ansible Playbook.



Using a Survey

When launching a job, the user will now be prompted with the Survey. The user can be required to fill out the Survey before the Job Template will execute.



What is threat hunting?

Threat hunting

Proactively defend your environment

What is threat hunting?

- Proactive tasks such as triage, identifying new threats.
- Updates from security bulletins and signature manipulation
- Correlation of events to create new alerts
- Typically performed by security operators and analysts
- Requires multiple tools.

Lab Scenario

- You're the security operator in detect a firewall policy violation
- Then, we are the security analyst who needs to correlate events and investigate

Threat hunting
Scenario overview

Threat Hunting

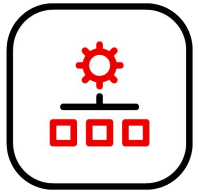
DDOS attack started

Analyst

opsids

opsfirewall

SIEM



Automation controller

Attacker

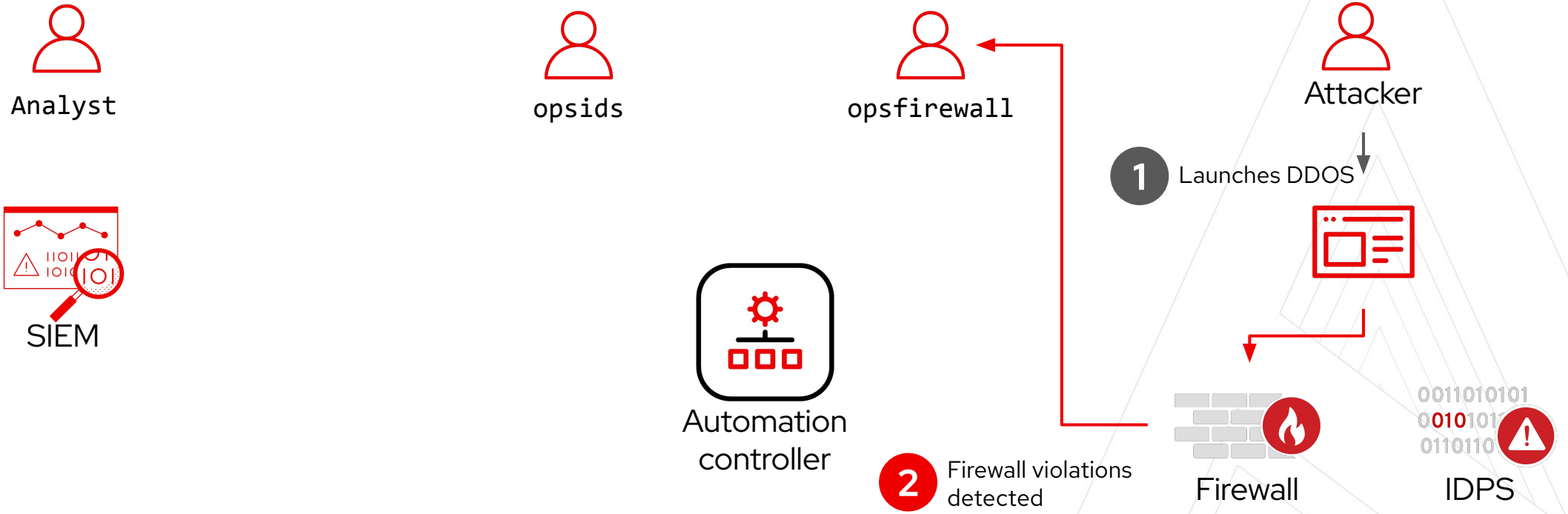
1 Launches DDOS

Firewall

IDPS

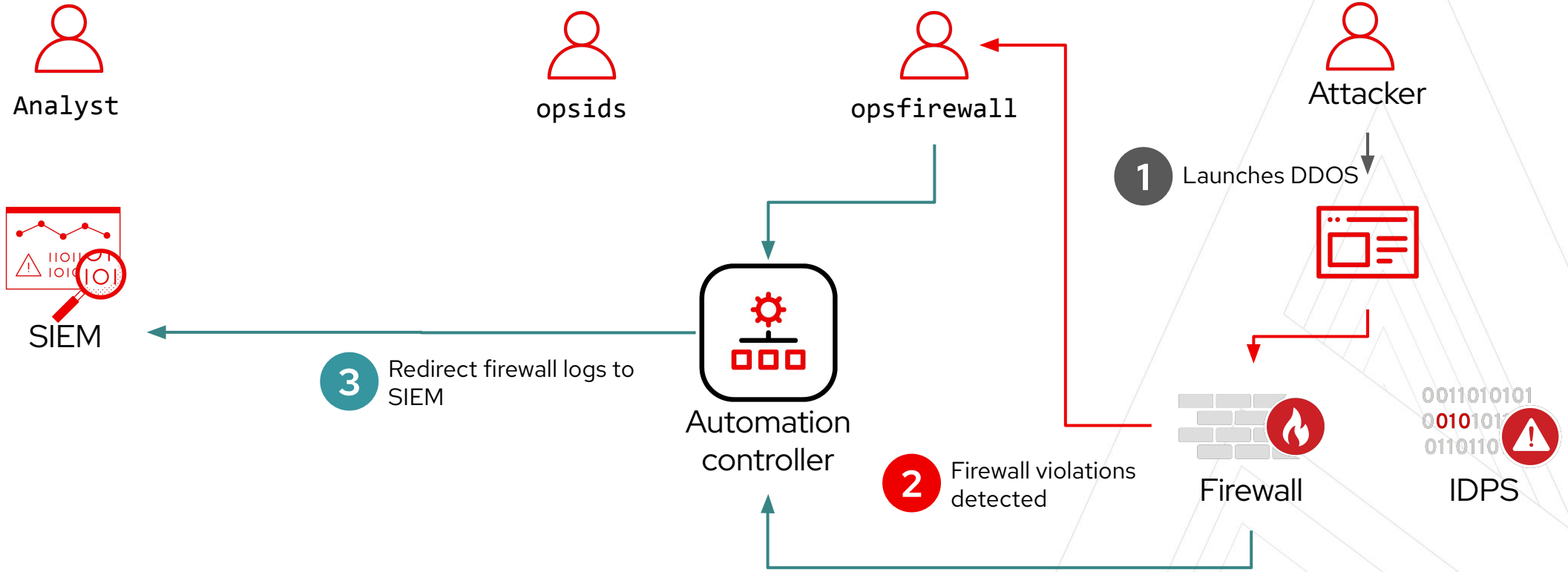
Threat Hunting

Firewall policy violated



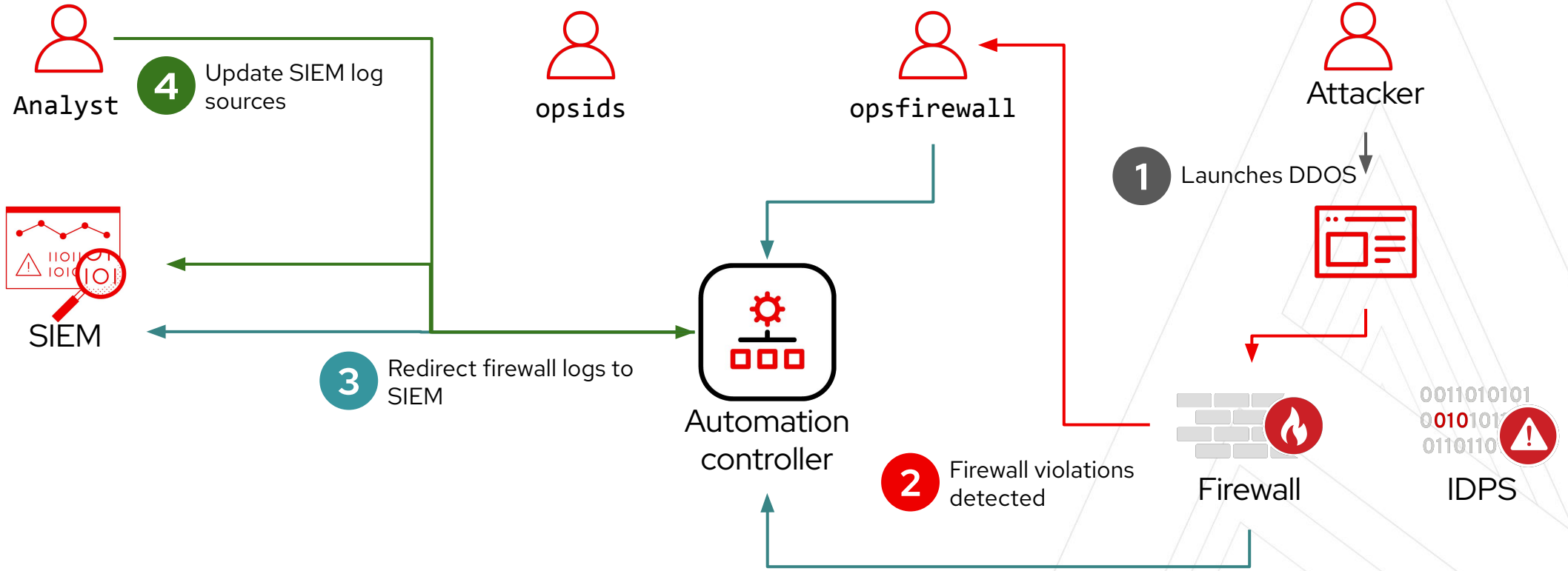
Threat Hunting

`opsfirewall` redirects logs to SIEM using controller



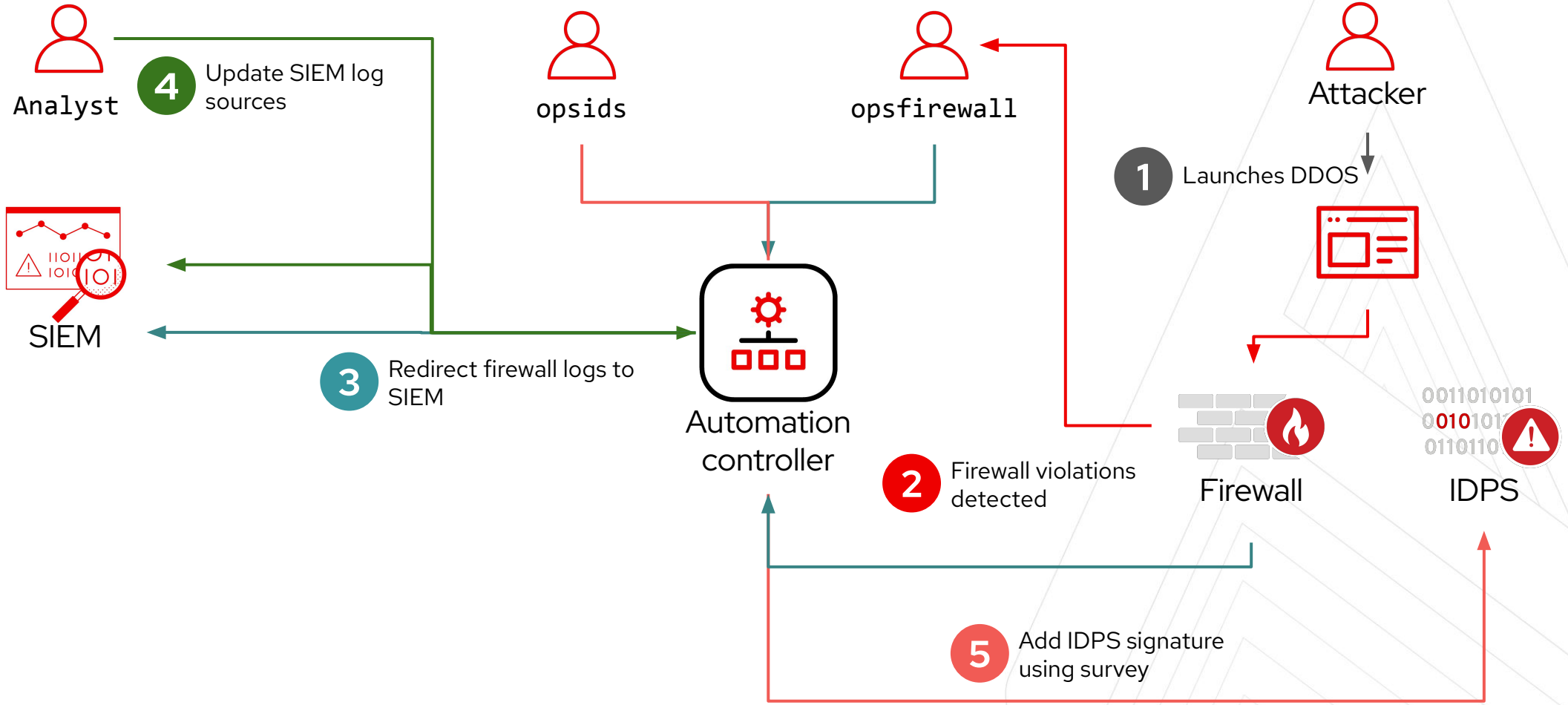
Threat Hunting

`analyst` updates QRadar log sources to accept firewall logs



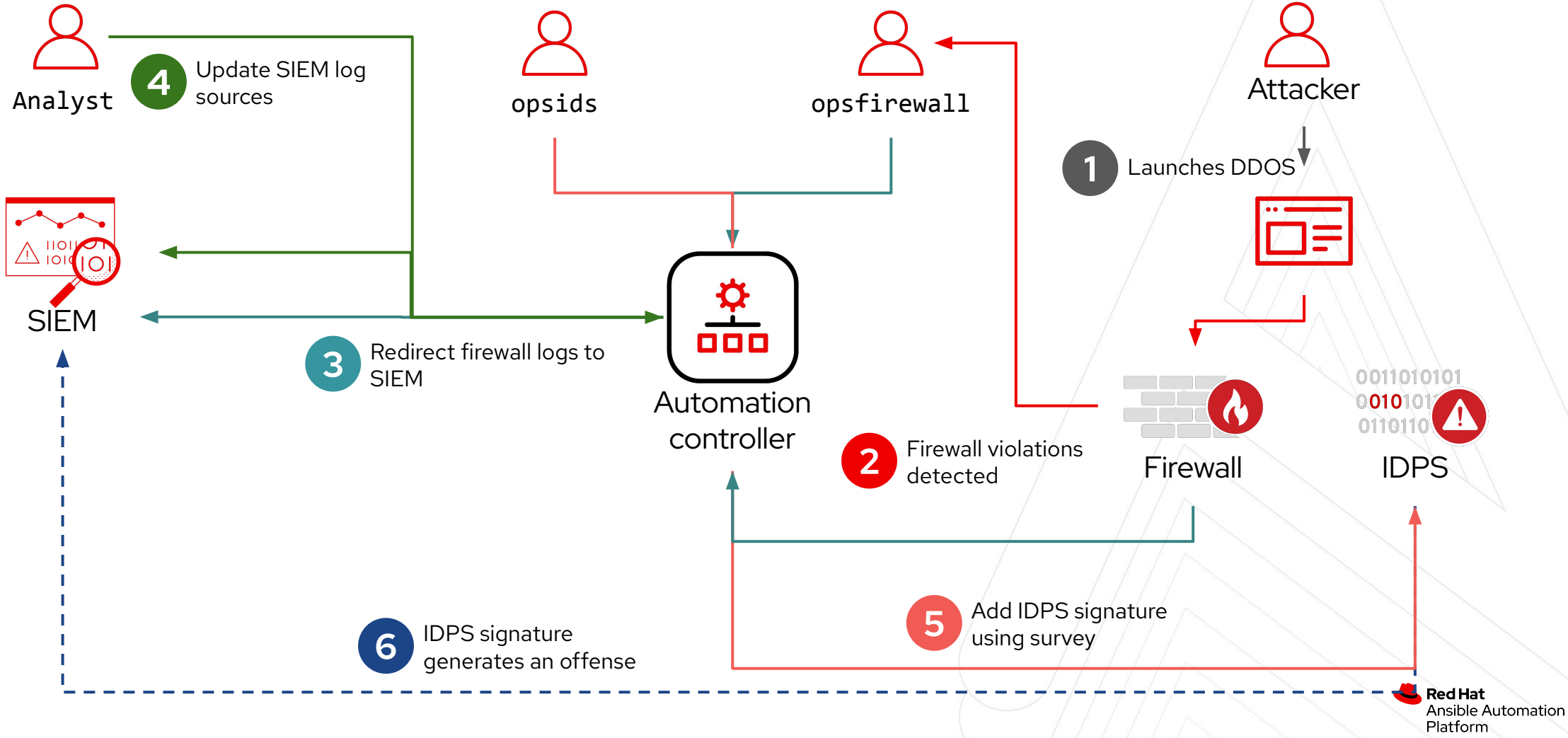
Threat Hunting

`opsids` adds IDPS signature using controller survey



Threat Hunting

IDPS signature generates an offense in the SIEM



Exercise Time!

Do Exercise 2.2 in your lab environment

- Follow the steps in the exercises
- Remember to use the IP addresses assigned to you

Exercise 2.3

Topics Covered:

- What is incident response?
- Lab scenario overview

Incident response

Mitigating the damage of a security attack or breach

What is incident response?

- Remediate a cyber attack or security breach
- Mitigate the risk caused by the security event
- Involves multiple stakeholders
- Organization must have incident response plan
- Requires multiple tools.

Lab Scenario

- As SecOps, we identify events generated on IDPS.
- Events need to be escalated. Logs must be redirects to SIEM
- As the analyst, we will inspect and create a remediation plan

Incident Response Scenario overview

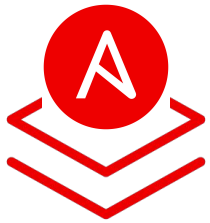
Incident Response

Attacker launches SQL injection attack

Analyst

SecOps

SIEM



Ansible Automation Platform

Attacker

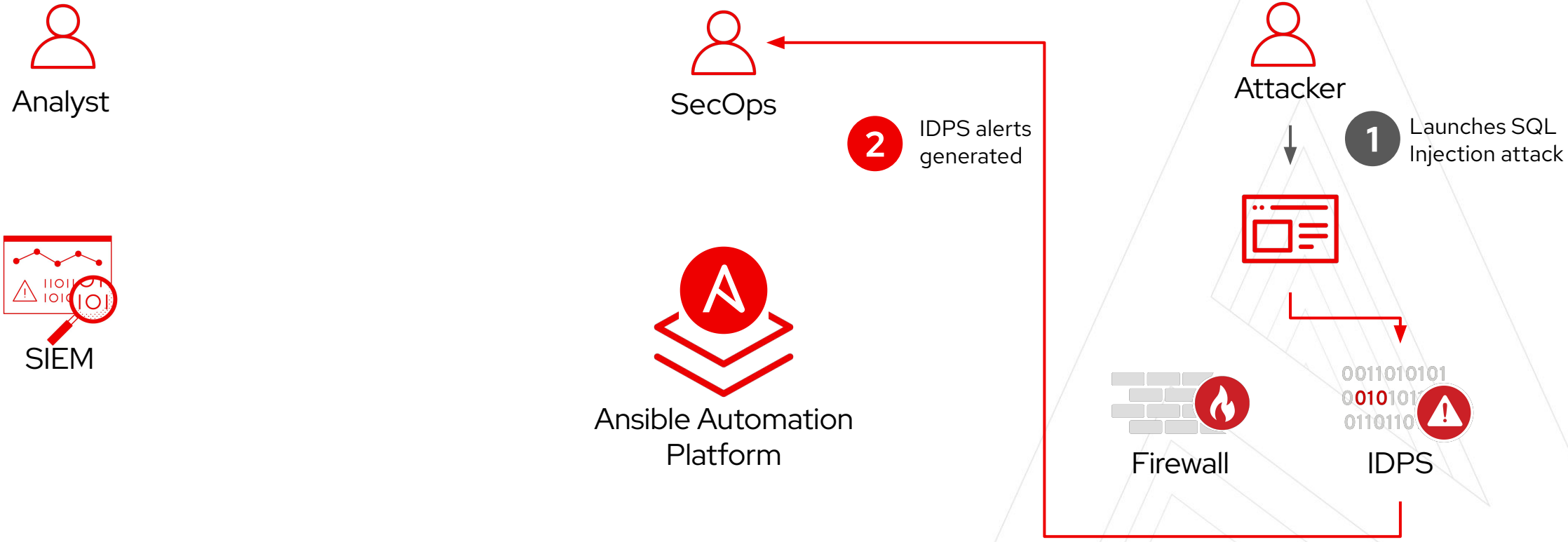
1 Launches SQL Injection attack

Firewall

IDPS

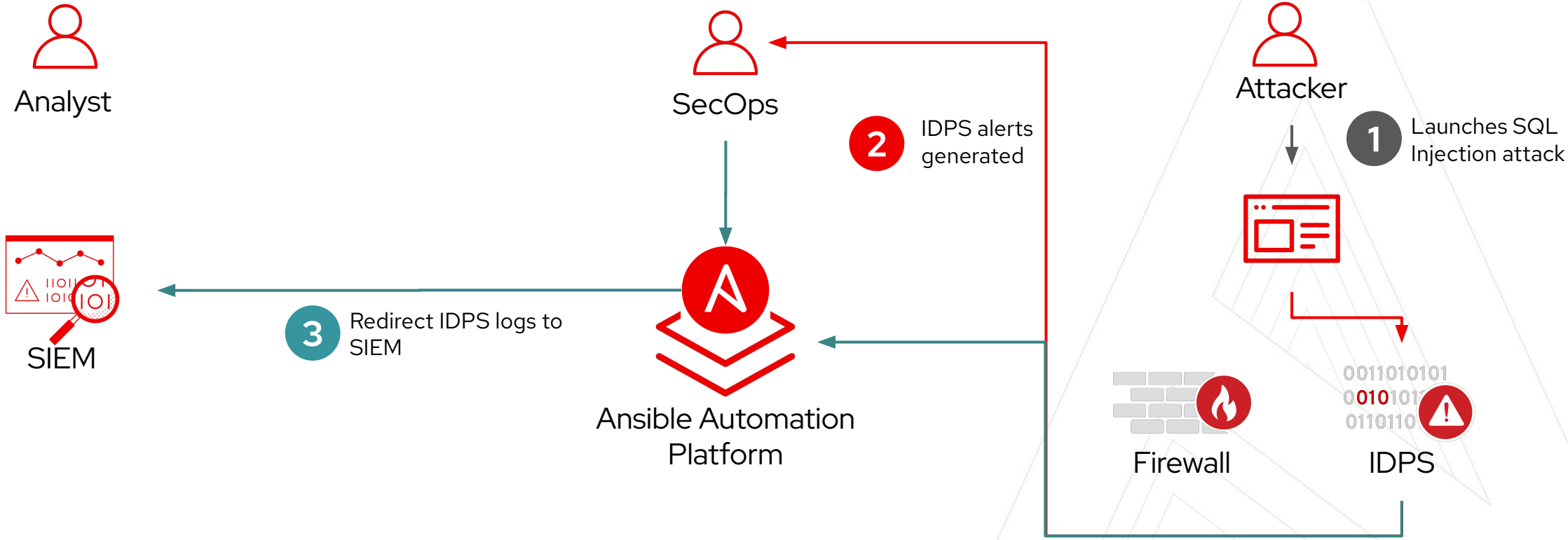
Incident Response

IDPS alerts identified by SecOps



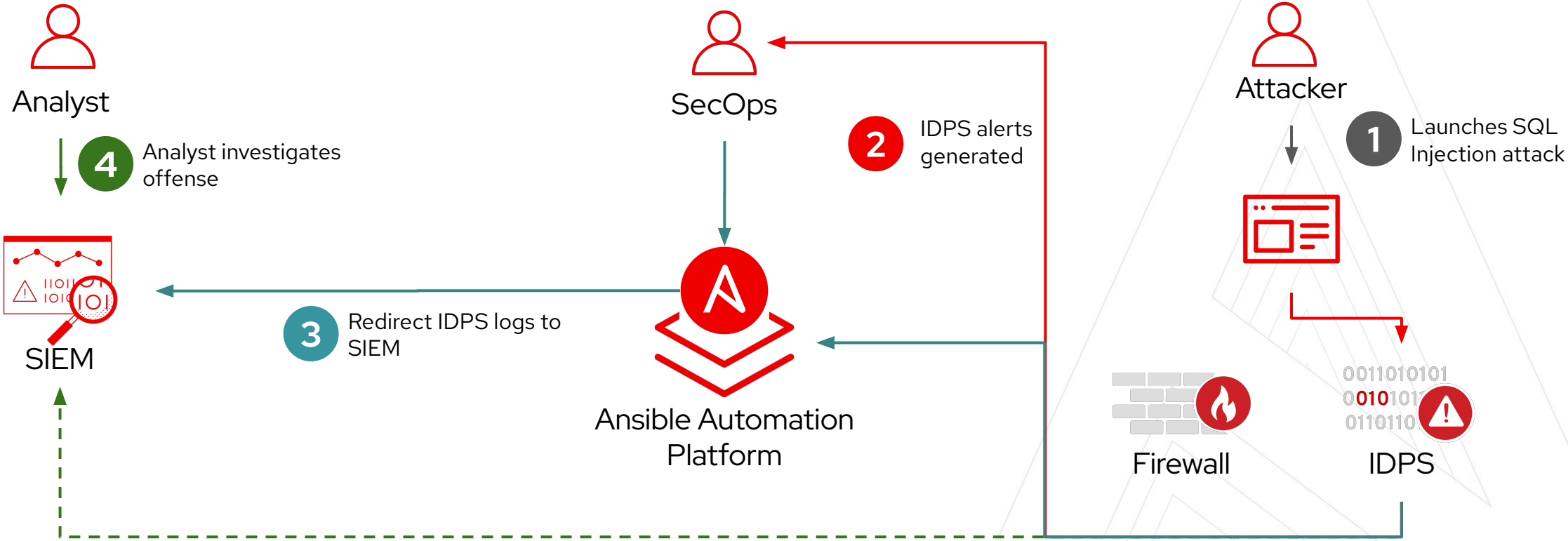
Incident Response

SecOps forwards events to SIEM



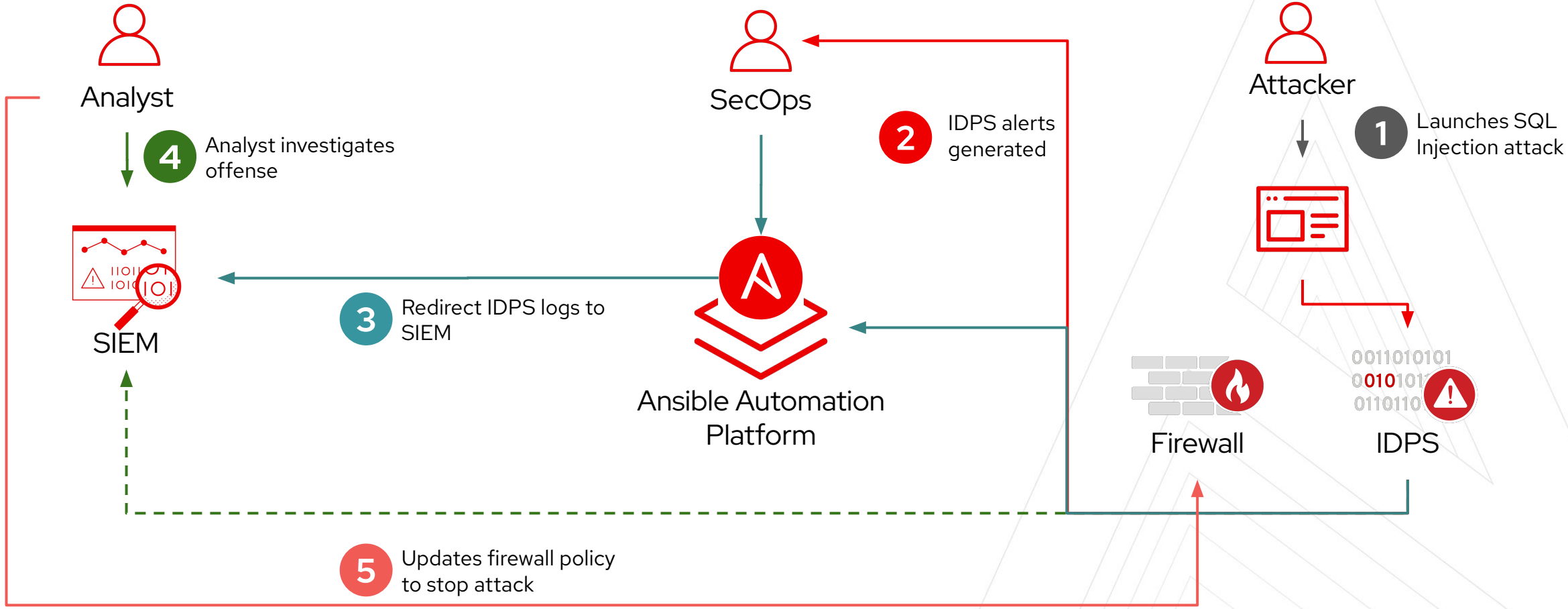
Incident Response

Analyst investigates offense generated on the SIEM



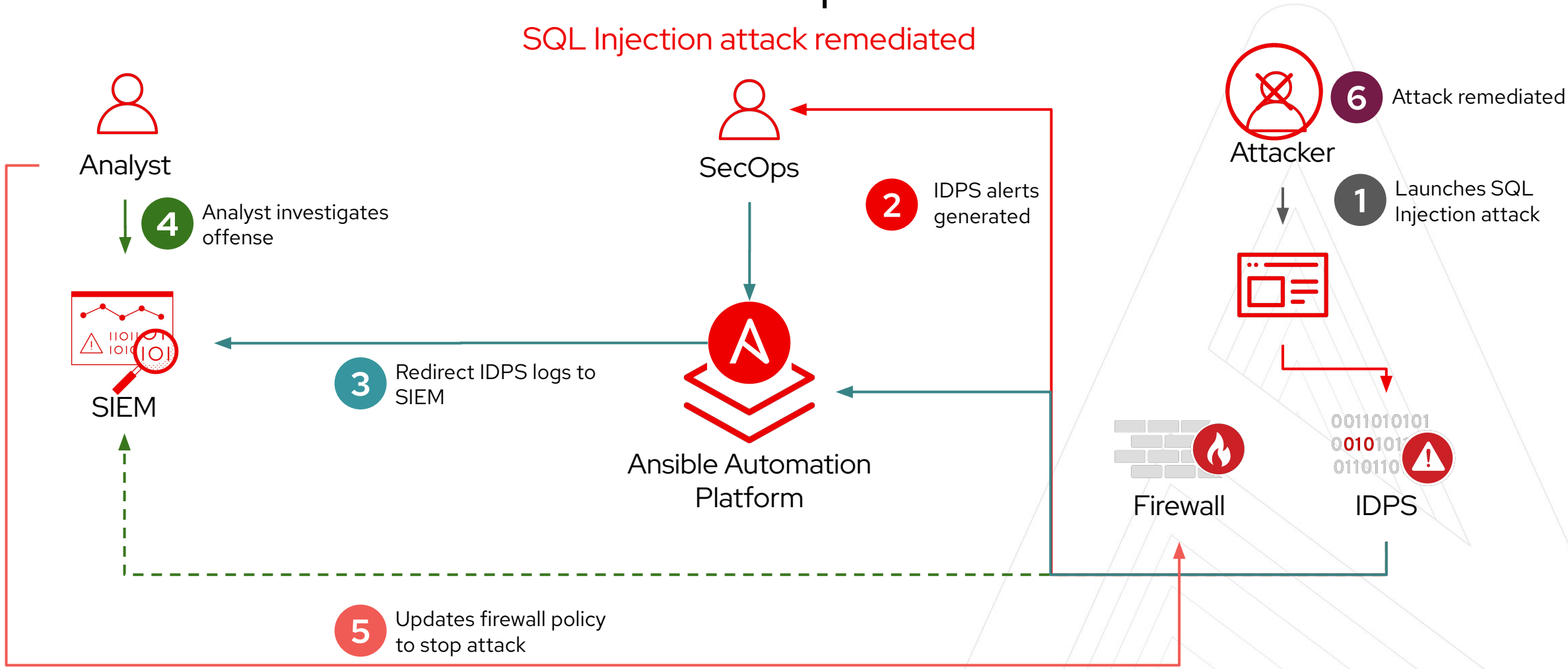
Incident Response

Analyst determines this is a cyber attack and launches remediation



Incident Response

SQL Injection attack remediated



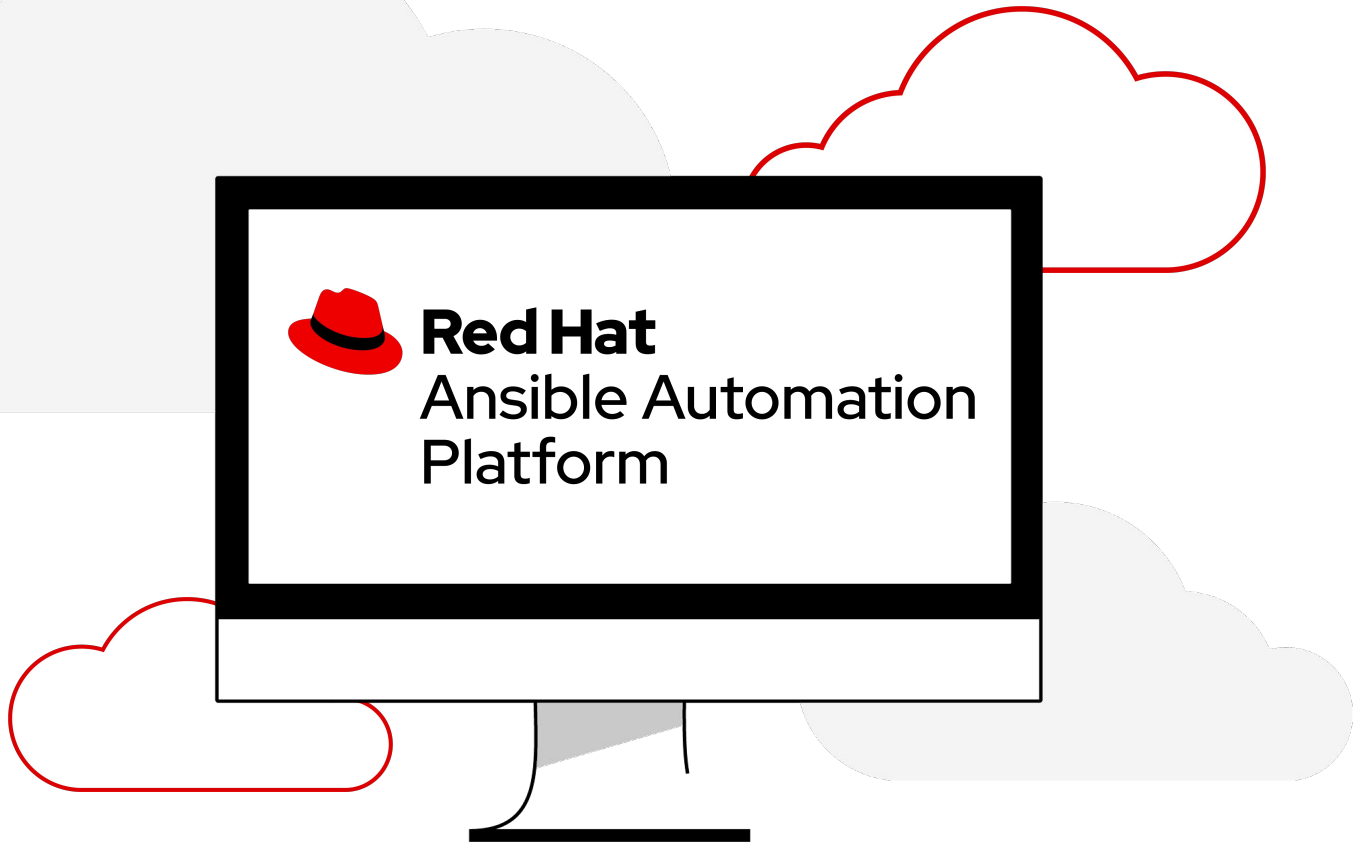
Exercise Time!

Do Exercise 2.3 in your lab environment

- Follow the steps in the exercises
- Remember to use the IP addresses assigned to you

Section 3

Wrapping up



Where to go next

Learn more

- Workshops
- Documents
- Youtube
- Twitter

Get started

- Trial subscription
- cloud.redhat.com

Get serious

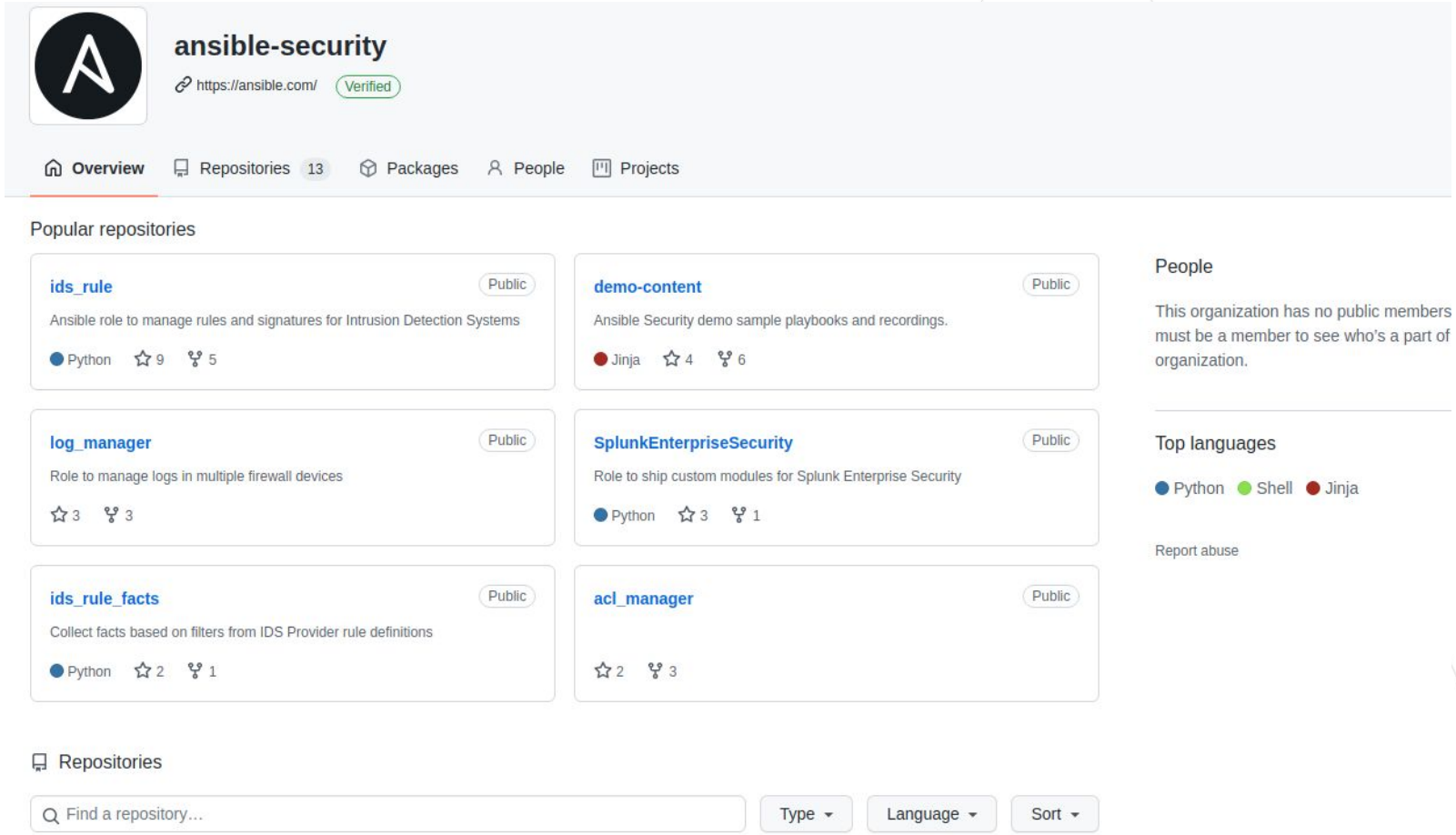
- Red Hat Automation Adoption Journey
- Red Hat Training
- Red Hat Consulting

Chat with us

- **Slack**
  Join by clicking here http://bit.ly/ansibleslack

Bookmark the Github organization

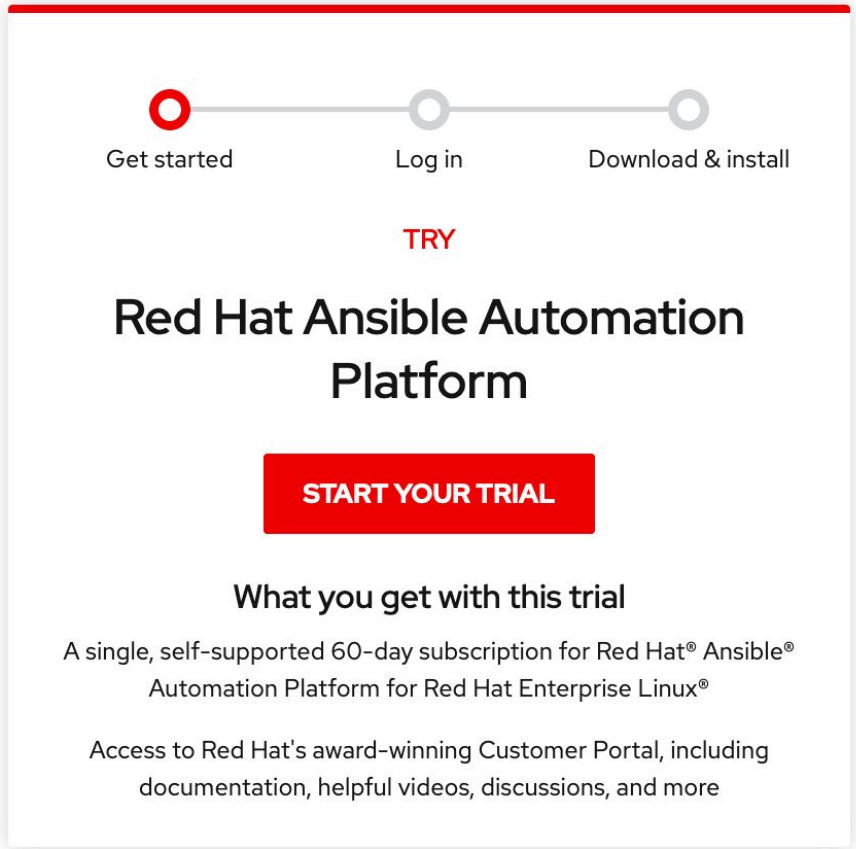
- GitHub organization
- Examples, samples and demos



Red Hat
Ansible Automation Platform

Resources

- Ansible Automation Platform website
- Ansible security automation (Overview)
- Simplify your security operations center (E-Book)
- Red Hat Ansible Automation Platform blog
- Start your Ansible Automation Platform trial



red.ht/ansible_trial

Red Hat
Ansible Automation Platform

Thank you

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat